**POLITYKA OCHRONY DANYCH OSOBOWYCH**
**OBOWIĄZUJĄCA W SF – FILTER sp .z o.o.**

**Lipiec 2024 r.**

SPIS TREŚCI

## WPROWADZENIE

Niniejszy dokument opisuje reguły oraz procedury dotyczące sposobu przetwarzania oraz bezpieczeństwa przetwarzania Danych Osobowych, w tym przetwarzania danych z użyciem systemów informatycznych przez Administratora Danych Osobowych tj. SF- FILTER sp. z o.o. z siedzibą w Lubinie, ul. Towarowa 10, 59-300 Lubin, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Wrocławia Fabrycznej we Wrocławiu, IX Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000264351, NIP: 6922418716, REGON: 020376416, kapitał zakładowy: 200 000, 00 zł. Dokument ma zastosowanie do przetwarzania wszelkich Danych Osobowych gromadzonych przez Administratora Danych Osobowych, pobieranych bezpośrednio od osób, których Dane dotyczą, a także z innych źródeł:

- pobieranych:
    - przez pracowników i współpracowników,
    - za pośrednictwem strony internetowej/stron internetowych: www.sf-filter.com , w tym poprzez formularz kontaktowy,
    - za pośrednictwem poczty elektronicznej, rozmów telefonicznych i poczty tradycyjnej przez – odpowiednio - adresy e-mail, numery telefonów i adresy wskazane na powyższej stronie internetowej,
    - za pośrednictwem social media, takich jak Facebook.
- Danych Osobowych, które Administrator Danych Osobowych przetwarza jako Podmiot przetwarzający,
- Danych Osobowych udostępnionych Administratorowi Danych Osobowych.

Polityka Ochrony Danych Osobowych określa przede wszystkim sposób postępowania w przypadku:

1. przetwarzania Danych Osobowych, niezależnie od tego z jakich źródeł Dane te pochodzą, w jakim celu są przetwarzane oraz jakich kategorii Danych Osobowych dotyczy przetwarzanie,
2. stwierdzenia naruszenia bezpieczeństwa ochrony Danych Osobowych,
3. stwierdzenia naruszenia zabezpieczenia systemów informatycznych, w jakich Dane są przetwarzane,
4. zapobiegania skutkom naruszenia bezpieczeństwa przetwarzania Danych Osobowych.

## ROZDZIAŁ I. PRZEPISY WPROWADZAJĄCE

### 1. DEFINICJE

Użyte w niniejszym dokumencie określenia oznaczają:

1.1. **Administrator Danych Osobowych (Administrator)** – SF- FILTER sp. z o.o. z siedzibą w Lubinie, ul. Towarowa 10, 59-300 Lubin, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Wrocławia Fabrycznej we Wrocławiu, IX Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000264351, NIP: 6922418716, REGON: 020376416, kapitał zakładowy: 200 000, 00 zł.

1.2. **Dane Osobowe (Dane)** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. W tym dane szczególnej kategorii, o których mowa w art. 9 ust. 1 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby,

1.3. **Hasło** – ciąg znaków składający się ze znaków literowych, cyfrowych, specjalnych lub innych, używany zazwyczaj podczas logowania do różnego rodzaju zasobów, m.in. systemów operacyjnych, baz danych, portali, poczty e-mail itp.,

1.4. **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną w danym systemie informatycznym, bazie danych, portalu, poczty e-mail itp.,

1.5. **Integralność** – właściwość zapewniająca, że Dane Osobowe są spójne, nie zostały zmienione, usunięte lub zniszczone w sposób nieautoryzowany,

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

1.7. **Polityka** – niniejsza Polityka ochrony Danych Osobowych,

1.8. **Poufność** – właściwość zapewniająca, że Dane Osobowe nie są udostępniane nieupoważnionym podmiotom. Jest rozumiana jako ochrona przed nieautoryzowanym ujawnieniem (odczytem) informacji osobom lub podmiotom trzecim, nieupoważnionym do ich uzyskania, bez uprzedniego upoważnienia (umocowania) na podstawie zgody, umowy lub na podstawie przepisów prawa,

1.9. **Pracownik** – osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także osoby współpracujące z Administratorem w oparciu o umowy cywilnoprawne (w szczególności: umowę zlecenia, umowę o współpracy lub o świadczenie usług), jeżeli wykonują usługi,

zlecenia lub dzieło na sprzęcie lub oprogramowaniu należącym do Administratora i przez niego udostępnionym,

1.10. **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania Danych Osobowych, które polega na wykorzystaniu Danych Osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Rozumie się przez to: 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 wpływa na jej sytuację (m.in. poprzez dopasowanie usług do tej osoby),

1.11. **Przetwarzanie Danych Osobowych** – operację lub zestaw operacji wykonywane na Danych Osobowych lub zestawach Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak m.in. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

1.12. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych, pełniący funkcję niezależnego publicznego organu nadzorczego w zakresie ochrony danych osobowych na terenie Rzeczpospolitej Polskiej,

1.13. **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),

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

1.15. **System Informatyczny** – system informatyczny, w którym Administrator przetwarza Dane osobowe, w tym oprogramowanie, aplikacje, poczta elektroniczna.

1.16. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

## 2. PODSTAWA PRAWNA

Polityka jest zgodna z następującymi aktami prawnymi:

2.1. Konstytucją Rzeczypospolitej Polskiej,

2.2. RODO,

2.3. Ustawą,

2.4. przepisami innych aktów prawnych powszechnie obowiązujących, w zakresie w jakim dotyczą ochrony danych osobowych.

## ROZDZIAŁ II. PODSTAWOWE ZASADY ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

### 1. ZAKRES OBOWIĄZYWANIA

1.1. Ochrona Danych Osobowych przetwarzanych przez Administratora obowiązuje wszystkie osoby, które mają dostęp do Danych Osobowych podlegających przetwarzaniu, bez względu na zajmowane stanowisko oraz miejsce wykonywania obowiązków służbowych, jak również charakter łączącej je z Administratorem umowy lub stosunku pracy.

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

1.3. Zachowanie tajemnicy (poufności) w zakresie Danych Osobowych obowiązuje zarówno podczas trwania stosunku pracy lub innej umowy łączącej Pracownika z Administratorem, jak również po ich ustaniu.

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

1.5. Polecenia Administratora, a także innych osób delegowanych i wyznaczonych do działań związanych z ochroną Danych Osobowych przez Administratora oraz w zakresie ochrony informacji i bezpieczeństwa Systemu Informatycznego, muszą być bezwzględnie wykonywane przez wszystkich Pracowników, którzy zajmują się przetwarzaniem Danych Osobowych.

### 2. ZASADY PRZETWARZANIA ORAZ OCHRONY DANYCH OSOBOWYCH

2.1. Zasady opisane poniżej obowiązują Administratora, jak i również jego Pracowników. W każdym opisanym poniżej przypadku, gdy jest odwołanie do postępowania Administratora, dotyczy to również zatrudnionych przez niego Pracowników.

2.2. Przetwarzanie Danych Osobowych przez Administratora może odbywać się wyłącznie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której Dane dotyczą.

2.3. Dane Osobowe zbierane są przez Administratora tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

2.4. Dane Osobowe mogą być przetwarzane przez Administratora w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.

2.5. Administrator zobowiązany jest do przetwarzania prawidłowych Danych i w razie potrzeby, szczególnie na wniosek osoby której Dane dotyczą, ich uaktualniania.

2.6. Dane Osobowe są 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.

2.7. Dane Osobowe są przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz

przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2.8. Dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe oraz do pomieszczeń, w których znajdują się serwery baz Danych Osobowych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają do tego odpowiednie upoważnienie udzielone przez Administratora lub zobowiązały się do zachowania poufności Danych, z którymi mogą się zapoznać w trakcie wykonywania usług lub innych czynności.

2.9. Przetwarzania Danych Osobowych może dokonywać wyłącznie osoba posiadająca upoważnienie do ich przetwarzania tj. osoba, która znajduje się w Ewidencji osób upoważnionych do przetwarzania Danych Osobowych stanowiącej Załącznik nr 8 do niniejszej Polityki.

## 3. PODSTAWA PRAWNA DO PRZETWARZANIA DANYCH OSOBOWYCH

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

3.1.1. osoba, której Dane dotyczą, wyraziła zgodę na przetwarzanie swoich Danych Osobowych w jednym lub większej liczbie określonych celów,

3.1.2. 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,

3.1.3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,

3.1.4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innej osoby fizycznej,

3.1.5. 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. Przetwarzanie Danych Osobowych szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO jest możliwe pod warunkiem, że:

3.2.1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych szczególnych,

3.2.2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą,

3.2.3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,

3.2.4. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą,

3.2.5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,

3.2.6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,

3.2.7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,

3.2.8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 9 ust. 3 RODO,

3.2.9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,

3.2.10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3.3. Administrator nie przetwarza Danych Osobowych, jeżeli nie spełni jednej z przesłanek, o których mowa w punktach poprzedzających.

3.4. Podstawy prawne przetwarzania Danych Osobowych przez Administratora, zostały wskazane w Rejestrze czynności przetwarzania danych osobowych, stanowiącym Załącznik nr 1 do Polityki.

## ROZDZIAŁ III. ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

### 1. PRZETWARZANIE DANYCH OSOBOWYCH

1.1. Administrator rejestruje przetwarzanie Danych Osobowych w rejestrze czynności przetwarzania, stanowiącym Załącznik nr 1 do niniejszej Polityki.

1.2. Administrator może również przetwarzać Dane Osobowe jako podmiot przetwarzający, na podstawie uprzednio zawartej umowie powierzenia danych osobowych. Wówczas odnotowuje istotne informacje na temat powierzenia Danych Osobowych do przetwarzania w rejestrze kategorii czynności przetwarzania, stanowiącym Załącznik nr 2 do niniejszej Polityki. Załącznik nr 2 powinien być aktualizowany zgodnie z obowiązującą treścią umowy powierzenia oraz poleceniami strony powierzającej Dane Osobowe.

### 2. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH ORAZ REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH PODMIOTU PRZETWARZAJĄCEGO

2.1. Rejestr czynności przetwarzania Danych Osobowych zawiera informację dotyczące czynności przetwarzania w zakresie:

2.1.1. danych identyfikujących Administratora, w tym jego nazwy oraz danych kontaktowych,

2.1.2. celów, w jakich są przetwarzane Dane Osobowe,

2.1.3. podstaw prawnych przetwarzania Danych Osobowych,

2.1.4. opisu kategorii osób, których Dane dotyczą, oraz kategorii Danych Osobowych,

2.1.5. kategorii odbiorców, którym Dane zostały lub zostaną ujawnione,

2.1.6. odnotowanie faktu przekazania Danych Osobowych do państwa trzeciego,

2.1.7. planowane terminy usunięcia poszczególnych kategorii Danych Osobowych,

2.1.8. ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa.

2.2. Rejestr kategorii czynności przetwarzania danych zawiera informacje dotyczące:

2.2.1 imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych,

2.2.2 kategorii przetwarzań dokonywanych w imieniu administratora wynikających z celu świadczonych usług lub zawartej umowy powierzenia,

2.2.3 odnotowanie faktu przekazania Danych Osobowych do państwa trzeciego,

2.2.4 jeżeli jest to możliwe - ogólnego opisu technicznego i organizacyjnego środków bezpieczeństwa,

2.2.5 gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji

międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO - dokumentacja odpowiednich zabezpieczeń.

## 3. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

3.1. Osoby, których dane osobowe są przetwarzane przez Administratora mogą skorzystać z uprawnień, przysługujących im na mocy art. 15-22 RODO, w postaci:

3.1.1. **Prawa dostępu do Danych.**

W przypadku otrzymania przez Administratora żądania dostępu do Danych Osobowych, Administrator oraz jego Pracownicy zobowiązani są:

3.1.1.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.1.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.1.3. a następnie zebrać i przedstawić tej osobie Dane, które Administrator przetwarza w formie zgodnej z treścią żądania lub ustalonej z tą osobą,

3.1.1.4. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

3.1.2. **Prawa przekazania kopii Danych.**

W przypadku uzyskania żądania przekazania kopii Danych od osoby, której dane dotyczą, Administrator oraz jego Pracownicy zobowiązani są:

3.1.2.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.2.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.2.3. skompletować te Dane i dostarczyć ich kopie w formie elektronicznej na adres e-mail wskazany przez ww. osobę lub dostarczyć kopię Danych w innej formie (zgodnie z treścią żądania),

3.1.2.4. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

Administrator nie pobiera opłat z tego tytułu w przypadku przekazania pierwszego egzemplarza kopii, zaś w przypadku kolejnych żądań tego typu od tej samej osoby, Administrator może pobierać opłaty odpowiadające realnym kosztom ich sporządzenia oraz dostarczenia, po uprzednim poinformowaniu o tym osoby składającej żądanie wraz ze wskazaniem wysokości opłaty i uzasadnieniem w zakresie ustalenia wysokości opłaty,

3.1.3. **Prawa do sprostowania lub aktualizacji Danych.**

W przypadku przekazania do Administratora żądania sprostowania lub uaktualnienia Danych Osobowych osoby, której Dane dotyczą, Administrator oraz jego Pracownicy zobowiązani są:

3.1.3.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.3.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.3.3. dokonać stosownych zmian w swoim Systemie Informatycznym, informując jednocześnie o tym osobę, której Dane dotyczą,

3.1.3.4. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

3.1.4. **Prawa do usunięcia Danych.**

W przypadku przekazania do Administratora żądania usunięcia Danych (prawo do bycia zapomnianym) przez osobę, której Dane dotyczą, Administrator oraz jego Pracownicy zobowiązani są:

3.1.4.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.4.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.4.3. sprawdzić czy mogą dokonać usunięcia danych i stosownie do sytuacji:

- usunąć lub zanonimizować Dane Osobowe dotyczące osoby składającej żądanie,
- pozostawić Dane informując tę osobę, że Administrator nie jest zobowiązany do ich usunięcia w związku z przepisem szczególnym lub spełnieniem spoczywającego na nim obowiązku prawnego (np. z uwagi na rozliczenia podatkowe, przedawnienie roszczeń lub realizację uprawnień z tytułu rękojmi lub gwarancji).

3.1.4.4. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

3.1.5. **Prawa do ograniczenia przetwarzania Danych.**

W przypadku przekazania do Administratora Danych Osobowych żądania dotyczącego ograniczenia przetwarzania Danych Osobowych przez osobę, której Dane te dotyczą, Administrator oraz jego Pracownicy zobowiązani są:

3.1.5.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.5.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.5.3. do ograniczenia przetwarzania tych Danych Osobowych do niezbędnego minimum, jeżeli żądanie jest uzasadnione, a Dane nie są niezbędne Administratorowi do realizacji umowy lub obowiązków prawnych,

3.1.5.4. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

3.1.6. **Prawa do przeniesienia Danych.**

W przypadku przekazania do Administratora Danych Osobowych żądania dotyczącego przeniesienia Danych Osobowych osoby, której Dane dotyczą, do innego administratora, Administrator oraz jego Pracownicy zobowiązani są:

3.1.6.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.6.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.6.3. do przekazania danych wskazanych przez osobę, której Dane dotyczą, w sposób rekomendowany przez tę osobę lub na wskazany przez tę osobę adres korespondencyjny, w sposób zapewniający odpowiednie bezpieczeństwo oraz poszanowanie pozostałych praw wynikających z przepisów powszechnie obowiązujących, o ile jest to technicznie możliwe,

3.1.6.4. w sytuacji, gdy nie jest to technicznie możliwe, osoba, której Dane dotyczą, otrzyma od Administratora dotyczące jej Dane Osobowe, w celu przekazania ich innemu Administratorowi bezpośrednio przez tę osobę,

3.1.6.5. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

3.1.7. **Prawo do sprzeciwu.**

Osoba, której dane dotyczą może w dowolnym momencie wnieść sprzeciw, wobec przetwarzania jej danych osobowych, opartego na art. 6 ust. 1 lit. e lub f RODO. W takim przypadku Administrator oraz jego Pracownicy są zobowiązani:

3.1.7.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.7.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.7.3. zaprzestać przetwarzania tych Danych, chyba że Administrator wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń – o czym poinformuje osobę, której Dane dotyczą,

3.1.7.4. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

3.1.8. **Prawo do cofnięcia zgody.**

Osoba, której Dane dotyczą ma prawo wycofać zgodę, będącą podstawą przetwarzania jej Danych w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. W takim przypadku Administrator oraz jego Pracownicy są zobowiązani:

3.1.8.1. upewnić się co do tożsamości osoby składającej żądanie,

3.1.8.2. w odpowiedzi na przyjęcie żądania spełnić wobec tej osoby obowiązek informacyjny (przedstawić właściwą klauzulę informacyjną),

3.1.8.3. usunąć lub zanonimizować Dane, chyba że dalsze przetwarzanie jest konieczne z uwagi na konieczność realizacji obowiązków prawnych nałożonych na Administratora lub jest uzasadnione z uwagi na prawnie uzasadniony interes Administratora, w postaci możliwości ustalenia, dochodzenia lub obrony roszczeń. Administrator informuje osobę, której Dane dotyczą o usunięciu Danych lub odmowie usunięcia,

3.1.8.4. postępować zgodnie z postanowieniami 3.2-3.17 poniżej.

3.2. Żądanie dotyczące wyżej opisanych w pkt 3.1.1. – 3.1.8. uprawnień może być złożone w formie wiadomości e-mail lub na piśmie (na adres korespondencyjny Administratora). Żądanie realizuje Administrator lub Pracownik wyznaczony przez Administratora. Realizacja żądania następuje nieodpłatnie, z zastrzeżeniem pkt 3.17.

3.3. Administrator lub wyznaczony przez niego Pracownik rejestruje każde otrzymane żądanie w rejestrze, którego wzór został określony w Załączniku nr 3 do Polityki. W tym celu każdy Pracownik zgłasza niezwłocznie, najpóźniej następnego dnia roboczego, wpływ żądania oraz jego przedmiot w wiadomości e-mail do bezpośredniego przełożonego lub Administratora.

3.4. Jeżeli Administrator lub Pracownik przez niego wyznaczony mają uzasadnione wątpliwości co do tożsamości osoby, której dane dotyczą, a która zgłosiła żądanie, o którym mowa w pkt. 3.1.1. – 3.1.6., mogą wystąpić do niej z żądaniem o potwierdzenie lub udokumentowanie swojej tożsamości m.in. poprzez weryfikację Danych Osobowych i informacji znajdujących się w posiadaniu Administratora.

3.5. W przypadku zgłoszenia żądania przez pełnomocnika osoby, której dane dotyczą, rozpoznanie żądania jest możliwe pod warunkiem, że przedstawi on pełnomocnictwo, z którego jednoznacznie wynika umocowanie do zgłoszenia żądania i zakres tego żądania.

3.6. W przypadku braku możliwości jednoznacznego określenia faktycznej treści żądania, Administrator lub Pracownik przez niego wyznaczony, mogą żądać od osoby zgłaszającej udzielenia dodatkowych wyjaśnień lub sprecyzowania żądania.

3.7. Przed udzieleniem odpowiedzi na żądanie Administrator lub Pracownik przez niego wyznaczony, weryfikują tożsamość osoby składającej żądanie, sprawdzając czy dane przedstawione w treści żądania są zgodne z danymi, które Administrator posiada w swojej bazie danych. W przypadku wątpliwości lub niezgodności danych osobowych Administrator lub Pracownik przez niego wyznaczony, kontaktują się telefonicznie lub mailowo w celu potwierdzenia tożsamości osoby składającej żądanie. Administrator może wówczas żądać dodatkowych informacji w celu potwierdzenia tożsamości osoby składającej żądanie.

3.8. Weryfikacja tożsamości odbywa się zgodnie z poniższymi zasadami:

3.8.1. w przypadku żądania od osoby zainteresowanej podania dodatkowych danych w celu jednoznacznego potwierdzenia tożsamości osoby składającej żądanie należy pozyskiwać jedynie dane w zakresie niezbędnym do osiągnięcia zamierzonego celu (np. prosząc o potwierdzenie informacji w zakresie danych, o których może mieć informacje składający żądanie),

3.8.2. w przypadku żądania od osoby składającej żądanie podania dodatkowych danych w celu jednoznacznego potwierdzenia jej tożsamości należy niezwłocznie, nie później niż w ciągu miesiąca, poinformować osobę składającą żądanie, że termin udzielenia odpowiedzi na żądanie będzie liczony od dnia udzielenia informacji umożliwiających jednoznaczną identyfikację,

3.8.3. w przypadku okazania przez osobę żądającą dokumentu w celu umożliwienia jednoznacznego potwierdzenia tożsamości dokument powinien być pozyskany wyłącznie do wglądu (nie powinna być wykonywana jego kopia lub skan).

3.9. Administrator (lub wyznaczony przez niego Pracownik) zobowiązany jest udzielić odpowiedzi na żądanie w terminie miesiąca od dnia jego otrzymania (wpłynięcia żądania do Administratora lub na skrzynkę mailową Pracownika Administratora). Jeżeli żądanie zostało skierowane w formie elektronicznej (wiadomość e-mail) odpowiedź na żądanie oraz pozostały kontakt w sprawie również prowadzony jest w formie elektronicznej (wiadomość e-mail) w tym samym wątku korespondencji, chyba że osoba składająca żądanie wyraźnie wskaże formę udzielenia odpowiedzi na żądanie. W przypadku żądania na piśmie, odpowiedź również udzielana jest w

formie pisemnej na adres wskazany przez żądającego, chyba że co innego wynika z treści żądania.

3.10. W przypadku zamiaru przesłania odpowiedzi drogą pocztową odpowiedź jest wysyłana nie później niż w terminie 3 dni roboczych przed upływem miesiąca od daty otrzymania żądania.

3.11. Jeżeli koniec terminu przypada na dzień ustawowo wolny od pracy, za ostatni dzień terminu uważa się najbliższy dzień roboczy.

3.12. W przypadkach otrzymania żądania, w związku z którym konieczne jest:

3.12.1. ustalenie lub weryfikacja tożsamości osoby zgłaszającej żądanie,

3.12.2. ustalenie lub doprecyzowanie przedmiotu żądania,

- miesięczny termin dotyczy podjęcia przez Administratora (lub wyznaczonego Pracownika) czynności w celu uzyskania informacji niezbędnych do ustalenia powyższych okoliczności. W taki przypadku termin na udzielenie odpowiedzi na żądanie wynosi miesiąc od dnia uzyskania przez Administratora wszystkich informacji niezbędnych do realizacji żądania, w tym przede wszystkim potwierdzenia tożsamości osoby składającej żądanie.

3.13. W sytuacji gdy wniesione żądanie jest skomplikowane lub Administrator otrzymałby dużą liczbę żądań od jednej osoby, co powoduje, że zachowanie terminu, o którym mowa w pkt 3.9, nie jest możliwe, wówczas 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 osobie, która skierowała do niego żądanie, informację o przedłużeniu terminu udzielenia odpowiedzi na żądanie wraz z uzasadnieniem dotyczącym przyczyn przedłużenia terminu, zaś w terminie nie dłuższym niż dwa miesiące od dnia przekazania ww. informacji spełni żądanie osoby, której Dane dotyczą.

3.14. Jeżeli Administrator (lub wyznaczony Pracownik) nie podejmuje działań w związku z żądaniem, wówczas niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego (PUODO) oraz skorzystania ze środków ochrony prawnej przed sądem. Mimo niepodjęcia działań Administrator lub wyznaczony Pracownik niezwłocznie podejmują czynności w celu wykonania żądania.

3.15. Odmowa podjęcia działań w związku ze zgłoszonym żądaniem dopuszczalna jest wyłącznie w przypadku, gdy:

3.15.1. żądanie jest ewidentnie nieuzasadnione,

3.15.2. żądania są nadmierne, w szczególności gdy ich zgłaszanie ma charakter ustawiczny.

3.16. O odmowie podjęcia działań z uwagi na okoliczności wymienione w poprzednim punkcie Administrator informuje żądającego w terminie miesiąca od dnia otrzymania żądania.

3.17. Administrator może jednak rozpoznać żądanie opisane w pkt 3.15., zamiast wydania odmowy, po uprzednim pobraniu opłaty za rozpoznanie żądania w wysokości ustalonej przez siebie i odpowiednio uzasadnionej. Informację o opłacie za realizację żądań przesyła Administrator lub upoważniony pracownik żądającemu niezwłocznie po ustaleniu jej wysokości i wskazaniu rachunku bankowego do dokonania opłaty, jednocześnie prosząc o potwierdzenie w terminie nie krótszym niż 3 dni, że żądanie ma być wykonane odpłatnie. Wraz z potwierdzeniem

wykonania żądania osoba żądająca wykonania żądań jest zobowiązywana do przesłania potwierdzenia przelewu na wskazaną kwotę. W przypadku nieotrzymania przelewu Administrator jest uprawniony do odmowy realizacji żądania o czym informuje żądającego niezwłocznie.

## 4. OBOWIĄZEK INFORMACYJNY (KLAUZULA INFORMACYJNA I POLITYKA PRYWATNOŚCI)

4.1. Przy pierwszym kontakcie z osobą, której dane przetwarza Administrator, a także w sytuacjach wprost wskazanych w Polityce, Administrator realizuje obowiązek informacyjny, o którym mowa w art. 13 lub 14 RODO, poprzez przedstawienie odpowiednich klauzul informacyjnych osobie, której Dane dotyczą, w formie elektronicznej lub papierowej. W przypadku użytkowników stron internetowych Administrator przedstawia im politykę prywatności, którą publikuje na swojej stronie internetowej.

4.2. Obowiązek informacyjny Administratora obejmuje przedstawienie informacji takich jak:

4.2.1. tożsamość i dane kontaktowe Administratora,

4.2.2. dane kontaktowe Inspektora Ochrony Danych (jeśli został wyznaczony),

4.2.3. cele przetwarzania Danych Osobowych oraz podstawa prawna tego przetwarzania,

4.2.4. prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią,

4.2.5. informacje o odbiorcach Danych Osobowych lub o kategoriach odbiorców, jeżeli istnieją,

4.2.6. informacje o zamiarze przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej,

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

4.2.8. 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,

4.2.9. informacja o prawie do cofnięcia zgody udzielonej przez osobę, której Dane dotyczą, w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

4.2.10. 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,

4.2.11. 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.

4.3. Obowiązek informacyjny Administrator spełnia przez przekazanie odpowiedniej klauzuli informacyjnej drogą elektroniczną lub przekazanie klauzuli informacyjnej jako załącznik do ofert lub umów zawieranych z osobami, których Dane dotyczą.

4.4. Administrator przekazuje obowiązek informacyjny osobom kontaktującym się drogą elektroniczną poprzez odesłanie właściwej klauzuli informacyjnej lub odesłanie do polityki prywatności opublikowanej na stronie internetowej Administratora.

4.5. Niedopuszczalnym jest niewypełnienie obowiązku informacyjnego przez Administratora lub jego Pracowników.

4.6. Obowiązek informacyjny spełniany jest również wobec osób, których Dane Osobowe zostały Administratorowi udostępnione. W takim przypadku treść obowiązku informacyjnego dostarczana jest osobie, której Dane dotyczą, po wejściu w posiadanie przez Administratora jej danych osobowych lub przy pierwszym kontakcie z osobą, której Dane dotyczą. Obowiązek informacyjny w zakresie wskazanym powyżej, przekazywany jest w formie elektronicznej, mailowej lub pisemnej. Obowiązek informacyjny Administratora powinien obejmować ujawnienie informacji takich jak:

4.6.1. tożsamość i dane kontaktowe Administratora oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe jego przedstawiciela,

4.6.2. dane kontaktowe Inspektora Ochrony Danych (jeśli został wyznaczony),

4.6.3. cele przetwarzania, do których mają posłużyć Dane Osobowe, oraz podstawę prawną przetwarzania,

4.6.4. kategorie odnośnych Danych Osobowych,

4.6.5. informacje o odbiorcach Danych Osobowych lub o kategoriach odbiorców, jeżeli istnieją;

4.6.6. gdy ma to zastosowanie – informacje o zamiarze przekazania Danych Osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz 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,

4.6.7. okres, przez który Dane Osobowe będą przechowywane, a gdy nie jest to możliwe - kryteria ustalania tego okresu,

4.6.8. jeżeli ma to uzasadnienie – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią,

4.6.9. 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,

4.6.10. 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,

4.6.11. informacje o prawie wniesienia skargi do organu nadzorczego (PUODO),

4.6.12. informacje o źródle pochodzenia Danych Osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

## 5. ANALIZA RYZYKA

5.1. Administrator przeprowadza analizę ryzyka w następujący sposób:

5.1.1. zarządzanie ryzykiem odnosi się do stopnia realizacji zasad ochrony Danych Osobowych oraz dotychczasowej praktyki i występujących zdarzeń u Administratora, które następnie podlegają oszacowaniu pod kątem ryzyka ich wystąpienia z zastosowaniem Metodyki szacowania ryzyka (pkt 5.2. poniżej),

5.1.2. okoliczności podane w pkt 5.1.1. są zidentyfikowane przez dokonującego analizę, a następnie poddane analizie, w tym przede wszystkim jakim zagrożeniom podlegają (na jakie zagrożenia są podatne) oraz jakie to niesie ze sobą skutki. Na tej podstawie szacowane jest ryzyko (w procesie szacowania ryzyka). Poziom ryzyka określa się w oparciu o iloczyn prawdopodobieństwa wystąpienia (P) oraz skutku wystąpienia (S) według następującego wzoru R (Ryzyko) = P (prawdopodobieństwo wystąpienia) x S (skutek),

5.1.3. następnie podejmowane są decyzje mające na celu obniżenie ryzyka do poziomu akceptowalnego (proces postępowania z ryzykiem). Wyniki obu w/w podprocesów należy dokumentować w Załączniku nr 4,

5.1.4. członkowie kadry kierowniczej są (w zakresie swoich kompetencji) odpowiedzialni za określenie listy potencjalnych zagrożeń wraz ze wskazaniem podatności systemu, uprawdopodobniających wystąpienie tych zagrożeń.

5.2. Metoda szacowania ryzyka przeprowadzana jest w następujący sposób:

5.2.1. arkusz analizy ryzyka zawiera 42 kategorie zdarzeń podlegających analizie, ocenie i oszacowaniu ryzyka w określonych grupach: zagrożenia podstawowe (w tym naruszenie zasad przetwarzania danych osobowych), zniszczenia fizyczne, utrata podstawowych usług, naruszenia bezpieczeństwa informacji, awaria techniczna, nieautoryzowane działania, naruszenia bezpieczeństwa funkcji. Zagrożenia sklasyfikowano przez wzgląd na lokalizację źródła zagrożenia (wewnętrzne lub/i zewnętrzne) oraz przyczynę zagrożenia (działania przypadkowe człowieka lub działania umyślne człowieka, przyczyna naturalna).

Skalę wystąpienia prawdopodobieństwa określono w następujący sposób:

- 1 - rzadkie
- 2 - mało prawdopodobne
- 3 - możliwe
- 4 - prawdopodobne
- 5 - prawie pewne

skalę skutku określono w następujący sposób:

- 1 - zdarzenie nie powoduje skutku
- 2 - zdarzenie wywołuje niewielki skutek
- 3 - zdarzenie wywołuje znaczący skutek
- 4 - zdarzenie wywołuje bardzo znaczący skutek

- 5 - zdarzenie wywołuje skutek katastrofalny

w zależności od udzielonych odpowiedzi wyróżnia się 5 poziomów wysokości ryzyka:

- 1 - 2 bardzo niskie
- 3 - 4 niskie
- 5 - 9 średnie
- 10 - 16 wysokie
- 17 - 25 bardzo wysokie

5.2.2. w przypadku wystąpienia ryzyka bardzo niskiego oznacza to, że przetwarzaniu nie zagraża naruszenie danych osobowych,

5.2.3. w przypadku wystąpienia ryzyka niskiego oznacza to, że przetwarzaniu nie zagraża znaczące naruszenie danych osobowych,

5.2.4. w przypadku wystąpienia ryzyka średniego istnieje prawdopodobieństwo wystąpienia naruszenia, które można zniwelować poprzez stosowanie się do rekomendacji wskazanych w Załączniku nr 4,

5.2.5. w przypadku wystąpienia ryzyka wysokiego oraz bardzo wysokiego, istnieje duże i bardzo duże prawdopodobieństwo wystąpienia naruszenia. W tej sytuacji Administrator zobowiązany jest do:

5.2.5.1. przeanalizowania sposobu przetwarzania danych osobowych w organizacji oraz sposobu jej działania,

5.2.5.2. przeprowadzenia oceny skutków dla ochrony danych osobowych, w odniesieniu do operacji, która zagrożona jest wysokim lub bardzo wysokim ryzykiem.

5.2.6. na podstawie wyników oceny ryzyka Administrator podejmuje decyzję o działaniach, które może zastosować w celu reagowania na ryzyko poprzez:

5.2.6.1. obniżenie ryzyka - wprowadzenie działań mających na celu obniżenie ryzyka do poziomu akceptowalnego. Do obniżenia poziomu ryzyka można wykorzystać następujące mechanizmy:

- organizacyjne (polityki, procedury, umowy),
- personalne (weryfikacja uprawnień, umowy o zachowaniu poufności),
- techniczne (system antywirusowe, firewall),
- fizyczne (systemy alarmowe, monitoring wizyjny).

5.2.6.2. akceptację ryzyka - podjęcie świadomej decyzji akceptacji zaistniałego poziomu ryzyka,

5.2.6.3. unikanie ryzyka - wyeliminowanie ryzyka poprzez zaprzestanie realizacji działań, które to ryzyko generują,

5.2.6.4. przeniesienie/podział ryzyka - polega np. na wykupieniu ubezpieczenia i ograniczenia w ten sposób skutków wystąpienia danego zdarzenia.

5.2.7. na podstawie przeprowadzonej oceny Administrator wydaje rekomendacje mające na celu zminimalizowanie środków ryzyka wiążącego się z przetwarzaniem danych osobowych,

5.2.8. Administrator zobowiązany jest do przeprowadzenia ponownej analizy ryzyka po wdrożeniu ww. rekomendacji.

5.3. Ponowna analiza ryzyka przeprowadzana jest co najmniej raz na rok, chyba że konieczność szybszego przeprowadzenia ponownej analizy wynika z:

5.3.1. z powodu zmian organizacyjnych lub prawnych, mających wpływ na zagrożenia i podatności,

5.3.2. z konieczności dokonania oceny skuteczności wdrożenia planu postępowania z ryzykiem, zgodnie z terminami określonymi w danym planie.

## 6. OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH

6.1. Administrator zobowiązany jest przeprowadzić ocenę skutków w przypadku:

6.1.1. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym Profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną, lub

6.1.2. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO, lub

6.1.3. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie,

6.1.4. gdy przeprowadzona analiza ryzyka wykazała, że istnieje wysokie lub bardzo wysokie ryzyko naruszenia ochrony danych osobowych.

6.2. Administrator zobowiązany jest także przeprowadzić ocenę skutków planowanych operacji przetwarzania Danych Osobowych w przypadku jednoczesnego wystąpienia co najmniej dwóch z poniższych operacji przetwarzania:

6.2.1. ewaluacja lub ocena, w tym Profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych,

6.2.2. zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki,

6.2.3. systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie, wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni (z wyjątkiem stosowania monitoringu wizyjnego, jeśli obraz nagrywany jest i wykorzystywany tylko w przypadku analizy incydentów naruszenia prawa),

6.2.4. przetwarzanie szczególnych kategorii danych osobowych i danych dotyczących wyroków skazujących i czynów zabronionych,

6.2.5. przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu,

6.2.6. przetwarzania danych genetycznych,

6.2.7. przetwarzanie danych osobowych na dużą skalę, gdzie pojęcie skali dotyczy: liczby osób, których dane dotyczą, zakresu przetwarzania, okresu przechowywania oraz geograficznego zakresu przetwarzania,

6.2.8. przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł,

6.2.9. przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi,

6.2.10. innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych w procesie przetwarzania,

6.2.11. przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usług lub umowy,

6.2.12. przetwarzanie danych lokalizacyjnych.

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

6.3.1. opis planowanych operacji przetwarzania Danych Osobowych i celów tego przetwarzania,

6.3.2. 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,

6.3.3. ocenę ryzyka naruszenia praw i wolności osoby, której Dane dotyczą, w szczególności, aby Administrator, jego pracownicy i współpracownicy zdawali sobie sprawę z ryzyka, jakie niesie wykorzystywana technologia,

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

6.4. Administrator przeprowadzi ocenę ryzyka w ramach Załącznika nr 5 do Polityki, jeśli zaistnieją przesłanki wskazane w pkt. 6.1.-6.2.

## ROZDZIAŁ IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

### 1. MOŻLIWE ZAGROŻENIA DOTYCZĄCE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1.1. Podział zagrożeń:

1.1.1. zagrożenia losowe zewnętrzne – ich występowanie może prowadzić do utraty Integralności Danych, ich zniszczenia i uszkodzenia, w tym uszkodzenia infrastruktury technicznej, służącej do przetwarzania Danych, np. klęski żywiołowe, przerwy w zasilaniu, utratę dostępu do systemów informatycznych, spowodowaną atakiem botów, itp.

1.1.2. zagrożenia losowe wewnętrzne – ich występowanie może prowadzić do zniszczenia Danych, zakłócenia ciągłości pracy Systemu Informatycznego oraz do naruszenia

Poufności Danych np. niezamierzone pomyłki operatorów, Administratora, Pracowników, podmiotu przetwarzającego, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania,

1.1.3. zagrożenia zamierzone – świadome i celowe działania powodujące naruszenie Poufności Danych, zazwyczaj nie skutkujące uszkodzeniem infrastruktury technicznej i zakłóceniem ciągłości pracy Systemu Informatycznego. Zagrożenia te można podzielić na:

1.1.3.1. nieuprawniony dostęp do Danych z zewnątrz (zarówno tych przetwarzanych w formie elektronicznej jak i tradycyjnej),

1.1.3.2. nieuprawniony dostęp do Danych wewnątrz organizacji (zarówno tych przetwarzanych w formie elektronicznej jak i tradycyjnej),

1.1.3.3. bezpośrednie zagrożenie sprzętu, na którym przetwarzane są Dane (np. kradzież sprzętu).

1.2. Naruszenie lub podejrzenie naruszenia ochrony Danych Osobowych, następuje w sytuacji:

1.2.1. losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby zawierające Dane jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne itp.,

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

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

1.2.4. pojawienia się odpowiedniego komunikatu alarmowego,

1.2.5. podejrzenia nieuprawnionej modyfikacji Danych znajdujących się w zasobach Administratora lub innego odstępstwa od stanu oczekiwanego,

1.2.6. naruszenia lub próby naruszenia Integralności Systemów Informatycznych,

1.2.7. pracy w Systemie Informatycznym wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony Danych Osobowych, jak np. praca osoby, która nie jest formalnie dopuszczona do obsługi danego systemu, programu,

1.2.8. ujawnienia nieautoryzowanych kont dostępu do systemów, programów, w których przetwarzane są Dane,

1.2.9. naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie Danych Osobowych w drukarce itp.).

1.2.10. niezabezpieczone pomieszczenia, w których przetwarzane są Dane,

1.2.11. niezabezpieczone urządzenia archiwizujące,

1.2.12. pozostawianie Danych w nieodpowiednich miejscach (m.in. w koszach na śmieci czy w miejscach publicznie dostępnych),

1.2.13. pozostawienie niezabezpieczonych dokumentów, zawierających Dane Osobowe na stanowisku pracy w razie jego opuszczenia przez osobę przetwarzającą Dane w imieniu Administratora.

## 2. POSTĘPOWANIE W PRZYPADKU PODEJRZENIA WYSTĄPIENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH (POSTĘPOWANIE WYJAŚNIAJĄCE)

2.1. W przypadku stwierdzenia podejrzenia naruszenia ochrony Danych Osobowych każda osoba zatrudniona lub współpracująca z Administratorem, zobowiązana jest do niezwłocznego powiadomienia bezpośredniego przełożonego oraz Administratora o wystąpieniu ww. zdarzenia.

2.2. Poza przypadkami określonymi w pkt. 2.1, za potencjalne naruszenie ochrony Danych Osobowych należy uznać wszelkie sytuacje prowadzące do naruszenia Poufności, Integralności lub dostępności Danych, w szczególności:

2.2.1. ujawnienie Danych Osobowych osobie nieuprawnionej (np. wysyłka dokumentów niezabezpieczonych hasłem na błędny adres e-mail),

2.2.2. wysyłka grupowej korespondencji elektronicznej z ujawnieniem Danych wszystkich odbiorców (niezastosowanie opcji ukrytej kopii),

2.2.3. zgubienie/zniszczenie dokumentów lub sprzętu służbowego, na którym przetwarzane są Dane Osobowe,

2.2.4. atak hackerski,

2.2.5. naruszenie zabezpieczeń systemu, urządzeń lub oprogramowania,

2.2.6. kradzież, pożar, zalanie lub inne sytuacje losowe, prowadzące do utraty Danych Osobowych.

2.3. Po wystąpieniu lub wykryciu zdarzeń określonych w punkcie poprzedzającym Pracownik zobowiązany jest niezwłocznie przekazać przełożonemu oraz Administratorowi notatkę dotyczącą zdarzenia (preferowana forma: wiadomość e-mail). Notatka powinna zawierać:

2.3.1. informację jakiej kategorii osób i jakiej kategorii Danych Osobowych, dotyczy naruszenie,

2.3.2. informację o skali naruszenia (wskazanie ilości osób, których dotyczy naruszenie),

2.3.3. wskazanie źródła naruszenia (wewnętrzne czy zewnętrzne),

2.3.4. czas wystąpienia naruszenia oraz czas trwania naruszenia,

2.3.5. charakter naruszenia,

2.3.6. opis sytuacji wraz z podjętymi przez Pracownika czynnościami, o których mowa w pkt 2.4 poniżej.

2.4. Pracownik, który wykrył naruszenie powinien podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a także zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,

2.5. Po ujawnieniu naruszenia ochrony Danych Osobowych, Administrator, jego przedstawiciel lub osoba upoważniona przez Administratora:

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

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

2.5.3. ocenia wagę naruszenia ochrony danych osobowych, zgodnie z Załącznikiem nr 7,

2.5.4. jeżeli zachodzi taka potrzeba - zleca usuniecie występujących naruszeń,

2.5.5. jeżeli zachodzi taka potrzeba - w terminie 72 godzin powiadamia PUODO o zaistniałym naruszeniu,

2.5.6. jeżeli zachodzi taka potrzeba i nie występują przesłanki, które wykluczają konieczność powiadomienia - bez zbędnej zwłoki powiadamia osoby, których Dane dotyczą o wystąpieniu naruszenia,

2.5.7. jeżeli naruszenie dotyczy powierzonych danych osobowych – informuje administratora danych osobowych o zaistniałym naruszeniu, zgodnie z zawartą umową powierzenia.

2.6. W oparciu o przeprowadzone czynności oraz uzyskane informacje, Administrator lub osoba upoważniona dokumentuje zaistniały przypadek naruszenia w rejestrze naruszeń stanowiącym Załącznik nr 6 do Polityki. Dla każdego naruszenia odnotowanego w Załączniku nr 6, należy przeprowadzić ocenę wagi naruszenia, zgodnie z Załącznikiem nr 7.

2.7. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez Administratora.

2.8. Analiza, o której mowa w pkt 2.7. powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie osób lub podmiotów odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

2.9. 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 określonymi zasadami, wszczyna się postępowanie dyscyplinarne.

## 3. WSPÓŁPRACA Z PUODO ORAZ ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

3.1. Administrator zobowiązany jest do współpracy z PUODO.

3.2. Współpraca Administratora z PUODO dotyczy zgłaszania naruszeń, a także uprzednich konsultacji dotyczących właściwego przetwarzania Danych Osobowych.

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

3.4. Zgłoszenie naruszenia powinno zawierać co najmniej:

3.4.1. 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,

3.4.2. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych (jeśli został wyznaczony) lub oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji na temat naruszenia,

3.4.3. opisywać możliwe konsekwencje naruszenia ochrony Danych Osobowych,

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

3.5. Administrator zobowiązany jest zawiadomić bez zbędnej zwłoki osobę, której Dane dotyczą, o każdym przypadku naruszenia ochrony Danych jej dotyczących, szczególnie jeżeli incydent ten może powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

3.6. Zawiadomienie osoby, której Dane dotyczą, musi zawierać co najmniej:

3.6.1. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie punktu kontaktowego, który pozwoli uzyskać więcej informacji,

3.6.2. opisywać możliwe konsekwencje naruszenia ochrony Danych Osobowych,

3.6.3. 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.

3.7. Zawiadomienie nie jest konieczne jeżeli:

3.7.1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do Danych Osobowych, których dotyczy naruszenie, w szczególności chodzi o takie środki, jak pseudonimizacja (pkt 3.8) oraz anonimizacja (pkt 3.9) Danych. Stosowanie tych środków powoduje, że nawet naruszenie ochrony Danych nie spowoduje powstania dodatkowego obowiązku informacyjnego (zawiadomienia),

3.7.2. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której Dane dotyczą,

3.7.3. 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.

3.8. Administrator w celu zabezpieczenia w miarę możliwości stosuje technikę 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.

3.9. Administrator w miarę możliwości stosuje technikę 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 V. TRANSFER DANYCH OSOBOWYCH

### 1. POWIERZENIE DO PRZETWARZANIA DANYCH OSOBOWYCH (UMOWA POWIERZENIA)

1.1. Administrator dopuszcza możliwość przekazania Danych Osobowych do przetwarzania innym Podmiotom przetwarzającym (podwykonawcom). W takim przypadku, przetwarzanie Danych Osobowych odbywa się wyłącznie na podstawie umowy powierzenia przetwarzania Danych Osobowych zawartej pomiędzy Administratorem, a Podmiotem przetwarzającym, zwanej dalej Umową.

1.2. Umowa musi być zawarta w formie umożliwiającej odtworzenie jej treści oraz zawierać ściśle określony zakres powierzonych do przetwarzania Danych.

1.3. Przetwarzanie Danych Osobowych możliwe jest wyłącznie w zakresie ustalonym w Umowie.

1.4. Powierzone Dane podlegają przetwarzaniu i ochronie na takich samych zasadach jakie stosuje Administrator, chyba że Umowa określi inne zasady ochrony Danych Osobowych.

1.5. Zmiana zasad związanych z ochroną Danych Osobowych oraz ich przetwarzaniem przez Podmiot przetwarzający, któremu Administrator powierzył Dane do przetwarzania nie może:

1.5.1. naruszać praw osób, których Dane są przetwarzane,

1.5.2. naruszać zasad związanych z ochroną Danych Osobowych przewidzianych w przepisach powszechnie obowiązujących,

1.5.3. zmieniać celu przetwarzania Danych Osobowych,

1.5.4. przetwarzać powierzonych Danych Osobowych w sposób inny niż w taki, do którego upoważnił go Administrator,

1.5.5. udostępniać powierzonych Danych Osobowych osobom trzecim bez zgody Administratora.

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

1.7. Podmiot przetwarzający:

1.7.1. zobowiązany jest zapewniać wszelkie środki wymagane do zapewnienia bezpieczeństwa przetwarzania Danych Osobowych,

1.7.2. w przypadku korzystania z podwykonawców przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (umowa podpowierzenia przetwarzania Danych Osobowych),

1.7.3. pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której Dane dotyczą,

1.7.4. po zakończeniu świadczenia usług związanych z przetwarzaniem – zależnie od decyzji Administratora – usuwa lub zwraca mu wszelkie Dane Osobowe oraz usuwa wszelkie ich istniejące kopie,

1.7.5. 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 administratorom, chyba że uzyska on zgodę osoby, której Dane dotyczą (z zastrzeżeniem pkt 2.2.) lub możliwość udostępnienia Danych Osobowych będzie wynikała z decyzji sądu, organu administracji publicznej lub nastąpi w oparciu o przepisy szczególne. Administrator może udostępniać Dane osobowe podmiotom trzecim, jeżeli jest to konieczne dla realizacji zawartych umów, a podmioty którym Dane są udostępniane, posiadają umocowanie do ich przetwarzania na podstawie obowiązujących przepisów prawa.

2.2. Administrator udostępnia Dane Osobowe Pracowników swoim kontrahentom, klientom i innym podmiotom, z którymi współpracuje celem wykazania reprezentacji oraz umożliwienia kontaktu w sprawie realizacji zawartych umów współpracy. Udostępnienie Danych Pracowników nie wymaga zgody. Dane Osobowe Pracowników udostępniane są na podstawie prawnie uzasadnionego interesu, jakim jest realizacja umów zawartych z podmiotami trzecimi. Dane udostępniane są wyłącznie w zakresie niezbędnym do wykazania prawidłowej reprezentacji Administratora podczas zawierania umów oraz do przeprowadzenia kontaktu związanego z realizacją zawartych umów.

2.3. W przypadku udostępniania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, Administrator zastosuje się do wymagań wynikających z przepisów powszechnie obowiązujących, a dotyczących udostępniania Danych Osobowych do państwa trzeciego, 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 lub określony sektor lub sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

3.2. Przekazanie Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić również, gdy Administrator oraz podmiot, któremu Dane przekazano, zapewnią odpowiednie zabezpieczenia i pod warunkiem, że zapewnione zostaną egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia można zapewnić – bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego – za pomocą:

3.2.1. wiążących reguł korporacyjnych zgodnie z art. 47 RODO,

3.2.2. standardowych klauzul ochrony Danych przyjętych przez Komisję Europejską zgodnie z procedurą sprawdzającą,

3.2.3. standardowych klauzul ochrony Danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską zgodnie z procedurą sprawdzającą,

3.2.4. 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,

3.2.5. 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 pkt. 3.1 oraz 3.2. niniejszego rozdziału, przekazywanie Danych Osobowych do państwa trzeciego może nastąpić pod warunkiem, że:

3.3.1. 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,

3.3.2. 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,

3.3.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której Dane dotyczą, między Administratorem a inną osobą fizyczną lub prawną,

3.3.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

3.3.5. przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,

3.3.6. 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,

3.3.7. 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 VI. ZABEZPIECZENIE DANYCH OSOBOWYCH

### 1. ŚRODKI FIZYCZNE

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

1.1.1. zabezpieczenie Danych przed ich udostępnieniem osobom nieupoważnionym,

1.1.2. zapobieganie przed pobraniem Danych przez osobę nieuprawnioną,

1.1.3. zapobieganie zmianie, utracie, uszkodzeniu lub zniszczeniu Danych,

1.1.4. zapewnianie przetwarzania Danych zgodnie z obowiązującymi przepisami prawa.

1.2. Zadania określone w punkcie poprzedzającym wykonuje lub nadzoruje ich wykonanie w imieniu Administratora Danych Osobowych.

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

1.3.1. samodzielny dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe, mają wyłącznie osoby mające odpowiednie upoważnienie nadane przez Administratora lub zobowiązane do zachowania poufności Danych Osobowych; osoby trzecie mogą przebywać w ww. pomieszczeniach wyłącznie w towarzystwie osoby upoważnionej,

1.3.2. pomieszczenia, w których przetwarza się Dane Osobowe, zamykane są na klucz,

1.3.3. w przypadku opuszczenia pomieszczenia przez ostatniego Pracownika upoważnionego do przetwarzania Danych Osobowych – także w godzinach pracy – Dane Osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (na zewnętrznych nośnikach np. pendrive, płyta CD/DVD) przechowywane są w miejscach zabezpieczonych przed dostępem nieupoważnionych osób trzecich; dodatkowo Pracownik w razie opuszczania swojego stanowiska pracy zobowiązany jest do wylogowania się ze swojego komputera stacjonarnego/laptopa lub innego urządzenia mającego dostęp do Danych Osobowych,

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

## 2. ŚRODKI TECHNICZNE

2.1. Zabezpieczenia przed nieautoryzowanym dostępem do Danych Osobowych następuje poprzez:

2.1.1. podłączenie urządzenia końcowego (komputera, drukarki) do Sieci Telekomunikacyjnej dokonywane jest przez Administratora lub osobę przez niego upoważnioną,

2.1.2. udzielenie Pracownikowi dostępu do Danych Osobowych, na podstawie upoważnienia do przetwarzania Danych Osobowych, którego wzór stanowi Załącznik nr 8 do Polityki,

2.1.3. identyfikację każdego Pracownika przetwarzającego Dane w Systemie Informatycznym Administratora, która następuje poprzez zastosowanie uwierzytelnienia (Identyfikatorem i Hasłem oraz w stosownych przypadkach uwierzytelnianiem dwustopniowym za pośrednictwem innego kanału kontaktu, np. poprzez uzyskanie kodu dostępu),

2.1.4. utworzenie każdemu Pracownikowi przetwarzającemu dane w Systemie Informatycznym konta z indywidualnym Identyfikatorem i Hasłem,

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

2.1.6. zabezpieczenie kont Hasłami,

2.1.7. ustalanie zakresu uprawnień konta Pracownika, zgodnie z nadanym mu upoważnieniem do przetwarzania Danych,

2.1.8. ustawienie monitorów stanowisk przetwarzania Danych Osobowych w sposób uniemożliwiający wgląd w Dane osobom nieupoważnionym.

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

2.2.1. stosowanie lokalnych list kontroli dostępu (ACL), skonfigurowanych na urządzeniach dostępowych, zainstalowanych w węzłach sieci WAN,

2.2.2. szyfrowanie sprzętowe lub programowe ruchu sieciowego, za pomocą którego przenoszone są informacje zawierające Dane Osobowe (szyfrowanie pomiędzy routerem węz a sieci WAN, a koncentratorem VPN w węźle centralnym sieci WAN),

2.2.3. separację centralnego węzła sieci Internet od sieci WAN za pomocą specjalizowanych urządzeń typu firewall (ASA),

2.2.4. separację węzła dostępu do instytucji zewnętrznych od sieci WAN za pomocą specjalizowanych urządzeń typu firewall (ASA).

2.3. Zabezpieczenia przed utratą Danych Osobowych w wyniku awarii:

2.3.1. ochrona sprzętu komputerowego przed zanikiem zasilania poprzez stosowanie listew przepięciowych lub urządzeń podtrzymujących napięcie (np. typu UPS lub przetworników odcinających zasilanie w przypadku spadku napięcia w sieci elektrycznej),

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

2.3.3. zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego.

## 3. PROCEDURY NADAWANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH

3.1. Wszyscy Pracownicy, którzy w zakresie swoich obowiązków przetwarzają Dane Osobowe, przed przystąpieniem do wykonywania ww. obowiązków muszą zostać przeszkoleni z zasad bezpiecznego przetwarzania danych osobowych oraz zapoznać się z niniejszą Polityką.

3.2. Fakt odbycia szkolenia oraz zapoznania się z niniejszą Polityką, Pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik nr 8 (Upoważnienie do przetwarzania Danych Osobowych wraz z klauzulą poufności).

3.3. W ramach Załącznika nr 8 Administrator wskazuje zakres upoważnienia do przetwarzania Danych.

3.4. Ewidencja osób upoważnionych do przetwarzania Danych Osobowych, wskazująca konkretnych Pracowników dopuszczonych do przetwarzania Danych Osobowych z określonych rejestrów, znajduje się Załączniku nr 9 do niniejszej Polityki.

3.5. Administrator Danych Osobowych (lub osoba przez niego wyznaczona) przyznaje uprawnienia dostępu do Systemu Informatycznego, określając zakres uprawnień Pracownika na podstawie upoważnień, o których mowa w pkt. 3.2.-3.3.

3.6. Administrator danych osobowych (lub osoba przez niego wyznaczona) zakłada konto Pracownika w Systemie Informatycznym, nadając mu indywidualny Identyfikator oraz umożliwia zabezpieczenie je Hasłem.

3.7. Hasło uprawniające do korzystania z Systemu Informatycznego Pracownik wpisuje osobiście.

3.8. Konto zostaje zablokowane lub usunięte przez Administratora lub osobę przez niego upoważnioną w przypadku zakończenia współpracy lub w momencie nieobecności dłuższej niż 30 dni.

3.9. Hasło dostępu Pracownika do Systemu Informatycznego stanowią tajemnicę służbową, znaną wyłącznie temu Pracownikowi.

3.10. Hasła, w stosunku do których zaistniało podejrzenie o ich ujawnieniu osobie nieuprawnionej, podlegają bezzwłocznej zmianie, po uprzednim zablokowaniu konta Pracownika.

3.11. W celu zabezpieczenia dostępu do Systemu Informatycznego, Administrator posiada hasło dostępu awaryjnego do Systemu.

## 4. ZASADY POSŁUGIWANIA SIĘ HASŁAMI

4.1. Bezpośredni dostęp do Systemu Informatycznego, może mieć miejsce wyłącznie po wprowadzeniu Identyfikatora i właściwego Hasła.

4.2. Za regularną zmianę Haseł w Systemie Informatycznym odpowiada Pracownik. Zalecana jest zmiana Hasła nie rzadziej niż co 90 dni.

4.3. Hasło powinno być zmieniane, szczególnie w sytuacjach, kiedy zaistnieje podejrzenie, iż jest ono znane osobom nieupoważnionym.

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

4.5. Pracownicy są odpowiedzialni za zachowanie Poufności swoich Identyfikatorów i Haseł.

4.6. Hasła utrzymuje się w tajemnicy również po upływie ich ważności.

4.7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że osoba nieupoważniona poznała Hasło w sposób nieuprawniony, Pracownik zobowiązany jest do natychmiastowej zmiany Hasła i poinformowania o zaistniałym fakcie Administratora.

4.8. Przy wyborze Hasła obowiązują następujące zasady:

4.8.1. minimalna długość Hasła to minimum 8 znaków;

4.8.2. zakazuje się stosować:

4.8.2.1. haseł, które Pracownik stosował uprzednio,

4.8.2.2. swojego Identyfikatora w jakiejkolwiek formie,

4.8.2.3. swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny),

4.8.2.4. ogólnie dostępnych informacji o Pracowniku (numer telefonu, numer rejestracyjny samochodu, numer PESEL itp.),

4.8.3. należy stosować:

4.8.3.1. hasła zwierające kombinacje liter (małych i dużych) i cyfr arabskich,

4.8.3.2. hasła zawierające znaki specjalne: (.,();'@, #, & itp.), o ile System Informatyczny i oprogramowanie na to pozwala;

4.8.4. zmiany Hasła nie wolno zlecać innym osobom.

## 5. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

5.1. Rozpoczęcie pracy w Systemie Informatycznym na komputerach Pracowników, wymaga zalogowania przy użyciu indywidualnego Identyfikatora oraz Hasła.

5.2. Przed opuszczeniem stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i Systemu Informatycznego .

5.3. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z Systemu Informatycznego.

5.4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania.

5.5. Wszystkie osoby przetwarzające Dane Osobowe z upoważnienia Administratora obowiązuje zasada „czystego biurka", zabraniająca pozostawiania jakichkolwiek dokumentów z Danymi Osobowymi podczas nieobecności pracownika przy stanowisku pracy. Niedozwolone jest pozostawianie dokumentacji papierowej z Danymi Osobowymi na stanowisku pracy po zakończeniu pracy. Dokumentacja powinna zostać zabezpieczona tak, aby uniemożliwić zapoznanie się z Danymi Osobowymi osobom nieuprawnionym.

5.6. W przypadku opuszczenia stanowiska pracy osoba przetwarzająca Dane Osobowe powinna wylogować się z Systemu lub zablokować dostęp do pulpitu stacji roboczej, z której korzysta przy przetwarzaniu Danych Osobowych. Ponadto w razie opuszczenia stanowiska pracy lub zakończenia pracy z Systemem Informatycznym, należy zamykać pliki zawierające Dane Osobowe. Uniemożliwi to dostęp do Danych Osobowych osobie nieupoważnionej (polityka czystego ekranu).

## 6. PROCEDURY TWORZENIA KOPII ZAPASOWYCH

6.1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator.

6.2. Kopie bezpieczeństwa Danych zgormadzonych na serwerze wykonywane są codziennie przez Administratora.

6.3. 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, podlegają zniszczeniu w stopniu uniemożliwiającym ich odczytanie, przede wszystkim poprzez używanie niszczarek lub zlecenie zniszczenia dokumentów specjalistycznym podmiotom zewnętrznym przy zachowaniu wymogów poufności danych oraz wymogów zabezpieczenia danych, co najmniej odpowiadających standardom przedstawionym w Polityce.

## 7. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED SZKODLIWYM OPROGRAMOWANIEM

7.1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową i anty-spyware.

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

7.3. Definicje wzorców wirusów aktualizowane są zgodnie z ustawieniami używanego oprogramowania antywirusowego.

7.4. Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia.

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

7.6. Administrator przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach, na których przetwarzane są Dane Osobowe, zgodnie z ustawieniami oprogramowania antywirusowego.

7.7. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania. W przypadku wykrycia szkodliwego oprogramowania sprawdzane jest stanowisko komputerowe, na którym wykryto problem oraz wszystkie posiadane przez Pracownika nośniki.

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

8.1. Dane Osobowe przetwarzane z użyciem Systemów Informatycznych mogą być udostępniane wyłącznie osobom uprawnionym, na podstawie uprzednio udzielonych upoważnień lub stosownych umów gwarantujących wysoki poziom zabezpieczeń.

8.2. Udostępnianie Danych Osobowych drogą korespondencji e-mail, odbywa się z zabezpieczeniem plików hasłem i przekazaniem hasła innym kanałem kontaktu niż droga mailowa (np. SMS lub komunikator internetowy).

8.3. Udostępnianie Danych Osobowych nie może być realizowane drogą telefoniczną.

## 9. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO

9.1. Przeglądy i konserwacja urządzeń:

9.1.1. przeglądy i konserwacja urządzeń są wykonywane w terminach określonych przez producenta sprzętu,

9.1.2. nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte,

9.2. Przegląd programów i narzędzi programowych składających się na System Informatyczny w tym m.in. aktualizacja baz zawierających Dane Osobowe, przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

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

## 10. POŁĄCZENIE DO SIECI TELEKOMUNIKACYJNEJ

10.1. Połączenie do Sieci Telekomunikacyjnej jest realizowane poprzez sieć przewodową i bezprzewodową z zastosowaniem następujących zasad ochrony:

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

10.1.2. każdy komputer posiadający dostęp do Sieci Telekomunikacyjnej posiada oprogramowanie antywirusowe chroniące przed złośliwym oprogramowaniem (anty-spyware) oraz zaporę sieciową (firewall),

10.1.3. osobie korzystającej z Sieci Telekomunikacyjnej zabrania się wchodzenia na strony niezgodne z prawem lub zawierające wirusy oraz programy szpiegujące (trojan, spyware),

10.1.4. połączenie z Siecią Telekomunikacyjną publiczną zabezpieczone jest przez moduł firewall działający na routerze sieciowym,

10.1.5. na każdym komputerze działa osobny firewall.

10.2. Zabronione jest połączenie z Siecią Telekomunikacyjną z niedziałającym lub niezaktualizowanym programem antywirusowym i firewallem lub ich brakiem.

## 11. KORZYSTANIE Z KOMPUTERÓW I URZĄDZEŃ PRZENOŚNYCH

11.1. Administrator dopuszcza możliwość pracy zdalnej.

11.2. Praca zdalna powinna być wykonywana wyłącznie na sprzęcie udostępnionym lub zatwierdzonym przez Administratora.

11.3. Pracownik zobowiązany jest chronić sprzęt udostępniony przez Administratora przed kradzieżą, zniszczeniem oraz dostępem osób trzecich.

11.4. Pracownik nie może wykorzystywać sprzętu udostępnionego przez Administratora do celów prywatnych, przede wszystkim Pracownik nie może samodzielnie instalować dodatkowych aplikacji lub oprogramowania bez zezwolenia Administratora.

11.5. Praca zdalna powinna być świadczona w miejscu, które zapewnia bezpieczne przetwarzanie Danych Osobowych przez uniemożliwienie ich ujawnienia na rzecz osób nieuprawnionych lub utraty integralności tych danych.

11.6. Administrator zapewnia Pracownikowi pomoc techniczną w bezpiecznym świadczeniu pracy zdalnej. Pomoc techniczna obejmuje w szczególności:

11.6.1. niezwłoczne reagowanie na zgłaszane przez pracownika zakłócenia w funkcjonowaniu środków komunikacji elektronicznej lub połączenia z systemem teleinformatycznym ADO,

11.6.2. pomoc w szybkim przywracaniu dostępu do danych osobowych poprzez regularne tworzenie kopii zapasowych,

11.6.3. zapewnienie oprogramowania stosowanego w systemie teleinformatycznym lub kompatybilnego z nim oraz jego regularne testowanie i aktualizowanie,

11.6.4. bieżące informowanie pracownika o nowych zagrożeniach związanych z przetwarzaniem danych podczas świadczenia pracy zdalnej.

11.7. Podczas pracy zdalnej Pracownik nie może przetwarzać Danych Osobowych w formie wydruków papierowych – chyba, że jest to uzasadnione charakterem powierzonych obowiązków. W takim wypadku Pracownik przetwarza dane w formie materialnej, wyłącznie przez czas niezbędny do wykonywania danego obowiązku, chroniąc materiały przed kradzieżą, zniszczeniem oraz dostępem osób trzecich. Po zakończeniu wykonywania obowiązków dokumenty należy zwrócić do biura, a wszelkie zbędne kopie zniszczyć za pomocą niszczarki.

11.8. Administrator prowadzi ewidencje dokumentów wydanych Pracownikom w formie papierowej, wzór ewidencji stanowi Załącznik nr 10 do Polityki.

11.9. Administrator dopuszcza możliwość przetwarzania Danych Osobowych za pośrednictwem smartfonów oraz tabletów, udostępnionych Pracownikom. W takim przypadku udostępniony sprzęt zabezpieczony jest hasłem lub kodem pin.

11.10. Każdy przypadek zniszczenia lub zgubienia sprzętu udostępnionego przez Administratora, należy traktować jako potencjalne naruszenie ochrony Danych Osobowych. W takiej sytuacji Pracownik zobowiązany jest poinformować Administratora lub bezpośredniego przełożonego o zaistniałym zdarzeniu, zgodnie z postanowieniami Rozdziału IV pkt. 2.

## ROZDZIAŁ VII. 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 wynikających z niniejszej Polityki Ochrony Danych Osobowych.
2. Administrator zobowiązuje się do przeprowadzania okresowych audytów bezpieczeństwa przetwarzania danych osobowych przynajmniej jeden raz w roku od momentu wdrożenia niniejszej Polityki.
3. Każdy Pracownik przed przystąpieniem do wykonywania obowiązków, zostaje przeszkolony pod kątem zasad przetwarzania Danych Osobowych oraz zapoznaje się z niniejszą Polityką. Dodatkowo celem utrwalenia zasad bezpiecznego przetwarzania Danych Osobowych oraz celem zwiększenia świadomości osób odpowiedzialnych za przetwarzanie Danych, Administrator prowadzi cyklicznie szkolenia dla Pracowników.

## ROZDZIAŁ VIII. POSTANOWIENIA KOŃCOWE

Polityka Ochrony Danych Osobowych obowiązuje od dnia 12. 09. 2024 2024 r.

Wszelkie zmiany procedur wynikających z niniejszej wymagają zatwierdzenia przez Administratora.

**SPIS ZAŁĄCZNIKÓW**

Załącznik nr 1. Rejestr czynności przetwarzania Danych Osobowych.

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

Załącznik nr 3. Rejestr żądań.

Załącznik nr 4. Analiza ryzyka

Załącznik nr 5. Ocena skutków planowanych operacji przetwarzania Danych Osobowych (wzór).

Załącznik nr 6. Rejestr naruszeń ochrony Danych Osobowych (wzór).

Załącznik nr 7. Ocena wagi naruszenia ochrony Danych Osobowych (wzór).

Załącznik nr 8. Upoważnienie do przetwarzania Danych Osobowych wraz z klauzulą poufności (wzór).

Załącznik nr 9. Ewidencja osób upoważnionych do przetwarzania Danych Osobowych.

Załącznik nr 10. Rejestr udostępnionych dokumentów.

Opracowane przez:
ENSIS Kancelaria Prawna Cioczek & Wspólnicy Sp. K.
ul. Żmigrodzka 81-83, lok.306, 51-130 Wrocław
NIP: 8971784540, KRS: 0001015831

SF-FILTER Sp. z o.o.
Wojciech Węcławek
Dyrektor Generalny
CZŁONEK ZARZĄDU