POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

w TERPA Sp. z o. o. Sp. k.

§ 1

1. Ilekroć w dokumencie jest mowa o:

a) **Administrator danych osobowych, ADO, TERPA, Administrator** – Terpa Sp. z o. o. Sp. k., ul. Pogodna 34, Lublin. Ilekroć mowa w niniejszej Polityce o czynnościach wykonywanych przez ADO rozumie się przez to działania Prezesa Zarządu TERPA.

b) **Dzieci lub małoletni** – dane osób poniżej 18 roku życia, chyba że Polityka stanowi inaczej

c) **Dane osobowe** – 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.

d) **Dane szczególnych kategorii** – dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

e) **Eksport danych** – przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

f) **IOD** – Inspektor Ochrony Danych wyznaczony przez ADO. Ilekroć mowa o IOD rozumie się również zastępcę IOD w rozumieniu przepisów Ustawy.

g) **Naruszenie** – naruszenie ochrony danych osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

h) **Odbiorca danych** – każdy podmiot, któremu ujawnia się dane osobowe.

i) **Państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.

j) **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

k) **Pracownik** - każdy osoba wykonująca pracę, zlecenie lub świadcząca usługi dla TERPA niezależnie od formy i rodzaju zawartej umowy. Przez pracownika rozumie się również wolontariusza, stażystę i praktykanta.

l) **Profilowanie** – dowolna forma 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.

m) **Przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak 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.

n) **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

o) **Rejestr** - rejestr czynności przetwarzania.

p) **Rozporządzenie lub 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).

q) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

r) **Środki techniczne i organizacyjne** – środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

s) **Ustawa** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

t) **Usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

u) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

v) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

w) **Zgoda** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 2

Każde przetwarzanie danych osobowych w TERPA odbywa się zgodnie z następującymi zasadami:

Przetwarzanie odbywa się zgodnie z przepisami prawa

TERPA jako administrator danych osobowych dba o to, aby przetwarzanie danych osobowych odbywało się zgodnie z przepisami prawa. TERPA odpowiedzialna jest w szczególności za właściwe projektowanie procesów przetwarzania danych osobowych oraz aktualizowanie wiedzy oraz poszerzanie świadomości pracowników w obszarze ochrony danych osobowych. Każda osoba dokonująca czynności na danych osobowych w imieniu TERPA zobowiązana jest upewnić się, czy istnieje legalna przesłanka przetwarzania danych osobowych.

Przetwarzanie odbywa się w sposób zapewniający bezpieczeństwo danych osobowych

TERPA odpowiedzialna jest za bezpieczeństwo procesów, pomieszczeń i rozwiązań informatycznych związanych z przetwarzaniem danych osobowych. Każda osoba dokonująca czynności na danych osobowych zobowiązana jest do stosowania środków ochrony danych osobowych ustanowionych w TERPA.

Przetwarzanie odbywa się w sposób zapewniający realizację praw osób, których dane dotyczą

TERPA odpowiedzialna jest za organizację procesów przetwarzania w taki sposób, aby były one realizowane w sposób przejrzysty dla osób, których dane dotyczą. Każda osoba dokonująca czynności na danych osobowych zobowiązana jest zweryfikować, czy wobec osób których dane dotyczą, został spełniony odpowiedni obowiązek informacyjny wynikający z przepisów RODO. Wszelkie żądania osób fizycznych dot. ich danych osobowych realizowane są bez zbędnej zwłoki.

Przetwarzanie odbywa się w sposób umożliwiających wykazanie przetwarzania zgodnie z prawem

TERPA odpowiedzialna jest za wykazanie, że dane osobowe przetwarzane są zgodnie z przepisami prawa. Każda osoba dokonująca czynności na danych osobowych zobowiązana jest dokumentować wszelkie czynności dokonywane na tych danych, z wyjątkiem czynności rutynowych lub dla których niniejsza Polityka wyznacza oddzielne reguły rozliczalności.

Przetwarzanie odbywa się w minimalnym zakresie niezbędnym do realizacji celu przetwarzania

Dane osobowe gromadzone w TERPA zbierane są jedynie w zakresie niezbędnym, do osiągnięcia celu dla którego zostały zebrane. Każda osoba dokonująca czynności związanych z odbieraniem danych osobowych od osób fizycznych, zobowiązana jest do ustalenia minimalnego zakresu niezbędnych do zebrania danych osobowych. Każdorazowo przed rozpoczęciem przetwarzania należy ustalić właściwy cel gromadzenia i przetwarzania danych.

Przetwarzanie odbywa się jedynie w czasie niezbędnym do realizacji celu przetwarzania

TERPA odpowiada za wyznaczenie stosownych ram czasowych przetwarzania danych osobowych. Dane osobowe przetwarzane są jedynie przez czas niezbędny do realizacji celu, dla którego zostały zebrane. Zbędne dane osobowe są niezwłocznie usuwane. Przechowywanie danych osobowych odbywa się zgodnie z terminami ustanowionymi w przepisach prawa, a w przypadku takich przepisów, jedynie gdy takie przechowywanie jest niezbędne do osiągnięcia celu, dla którego zostały zebrane.

Przetwarzanie odbywa się w sposób zapewniający prawidłowość danych

TERPA odpowiada za przetwarzanie danych osobowych w taki sposób, aby móc podejmować działania w przypadku gdyby dane okazały się nieprawidłowe w świetle celów ich przetwarzania. Dane nieprawidłowe podlegają sprostowaniu lub niezwłocznemu usunięciu.

§ 3

1. Wszelkie dane osobowe podlegają gromadzeniu pozwalającemu na ich identyfikacją, kategoryzację oraz wskazanie celów, do których zostały zebrane.
2. **Każda osoba odpowiedzialna za gromadzenie danych osobowych zobowiązana jest dokonać identyfikacji zasobów danych osobowych w szczególności z uwzględnieniem następujących informacji:**

a) kategorie danych osobowych,
b) przypadki przetwarzania danych szczególnej kategorii i danych o wyrokach skazujących,
c) przypadki przetwarzania danych osobowych małoletnich,
d) przypadki profilowania i przetwarzania danych w sposób zautomatyzowany
e) przypadki występowania wielu administratorów.

3. Przed każdą czynnością na danych osobowych należy upewnić się, czy istnieje podstawa prawna do przetwarzania danych. Każdorazowo należy skontaktować się z ADO lub IOD w celu ustalenia podstawy prawnej przetwarzania.
4. Prowadzony jest Rejestr czynności przetwarzania. Rejestr opracowuje, prowadzi i utrzymuje ADO. Rejestr służy identyfikacji procesów przetwarzania. Każda osoba odpowiedzialna za przetwarzanie danych osobowych zobowiązana jest upewnić się, czy dana czynność została ujęta w Rejestrze.

§ 4

1. ADO ma obowiązek stosować odpowiednie środki techniczne i organizacyjne, które zapewniają ochronę przetwarzanych danych osobowych, zgodnie z zagrożeniami oraz kategoriami danych. W szczególności ADO jest zobowiązany do zabezpieczenia danych przed:
   a) Udostępnieniem osobom nieupoważnionym,
   b) Zabraniem przez osobę nieuprawnioną,
   c) Przetwarzaniem z naruszeniem przepisów prawa,
   d) Zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. ADO zobowiązuje się do przestrzegania podstawowych zasad przetwarzania danych osobowych, które są zgodne z RODO, w szczególności:
   a) zgodność z prawem, rzetelność i przejrzystość - dane osobowe muszą być przetwarzane zgodnie z przepisami prawa, w sposób rzetelny i zrozumiały dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a RODO).
   b) ograniczenie celu - dane osobowe powinny być zbierane tylko w wyraźnie określonych, uzasadnionych celach i nie mogą być przetwarzane w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b RODO).
   c) minimalizacja danych - przetwarzane dane muszą być adekwatne, stosowne i ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c RODO).
   d) prawidłowość - dane osobowe muszą być prawidłowe i aktualizowane w razie potrzeby. ADO jest zobowiązany do usuwania lub korygowania nieprawidłowych danych (art. 5 ust. 1 lit. d RODO).

e) ograniczenie przechowywania - dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby przez okres nie dłuższy, niż jest to konieczne do celów, w których dane są przetwarzane (art. 5 ust. 1 lit. e RODO).

f) integralność i poufność - dane muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem, przy użyciu odpowiednich środków technicznych i organizacyjnych (art. 5 ust. 1 lit. f RODO).

3. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie nadane przez ADO. Wzór upoważnienia znajduje się w Załączniku nr 6 do niniejszej Polityki bezpieczeństwa.
4. ADO ma prawo w dowolnym momencie odwołać nadane upoważnienie, co również dokumentowane jest pisemnie. Wzór odwołania upoważnienia znajduje się w Załączniku nr 7.
5. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, a wzór ewidencji znajduje się w Załączniku nr 3.
6. ADO ponosi odpowiedzialność za bezpieczeństwo systemu informatycznego, w którym przetwarzane są dane osobowe. W szczególności zapewnia nadzór nad przestrzeganiem Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.
7. W przypadku naruszenia bezpieczeństwa systemu informatycznego lub innej formy przechowywania danych, ADO ma obowiązek sporządzić odpowiedni raport dotyczący incydentu, zgodnie z wymogami RODO. Raport zawiera w szczególności:
   a) data, godzina i miejsce incydentu,
   b) opis incydentu: zakres danych jaki podlegał naruszeniu, rodzaj naruszenia, systemy aplikacje lub bazy danych dotknięte incydentem.
   c) okoliczności wykrycia incydentu,
   d) osoby zaangażowane w wystąpienie incydentu, jeżeli są znane,
   e) podjęte działania w odpowiedzi na incydent,
   f) potencjalne skutki wystąpienia incydentu,
   g) działania naprawcze i zapobiegawcze,
   h) informacja o organach, którym został zgłoszony incydent,
   i) informacja, czy osoby których dane dotyczą, zostały poinformowane o wystąpieniu incydentu.
8. Raport o którym mowa w ust. 8 może powstać po konsultacji z IOD.

§ 5

1. **Wszyscy pracownicy TERPA są zobowiązani do przestrzegania postanowień zawartych w Polityce. W szczególności muszą oni zapewnić bezpieczeństwo danych osobowych przetwarzanych w ramach wykonywania swoich obowiązków.**
2. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy pracownik musi zapoznać się z przepisami dotyczącymi ochrony danych osobowych, w tym z postanowieniami Polityki. Potwierdzenie zapoznania się odbywa się poprzez podpisanie oświadczenia, którego wzór stanowi Załącznik nr 8 do niniejszej Polityki bezpieczeństwa. Oświadczenie to jest dołączane do akt pracowniczych lub innych dokumentów związanych ze stosunkiem prawnym pomiędzy pracownikiem i TERPA.
3. Pracownicy są odpowiedzialni za dbanie o bezpieczeństwo danych udostępnionych im do przetwarzania, archiwizowania lub przechowywania, zgodnie z Polityką. Do ich obowiązków należy w szczególności:
   a) pracownicy muszą zapewnić, że żadne dane nie będą dostępne dla osób, które nie mają uprawnień do ich przetwarzania,
   b) dane osobowe muszą być zabezpieczone przed przypadkowymi incydentami mogącymi spowodować ich uszkodzenie lub utratę.
   c) pracownicy są zobowiązani do ochrony wszelkich nośników danych osobowych (np. nośniki magnetyczne, optyczne, pamięci półprzewodnikowe, druki i wydruki) przed dostępem osób nieuprawnionych oraz przed przypadkowym zniszczeniem.
   d) pracownicy muszą zachować poufność dotyczącą haseł dostępu oraz wszelkich informacji technologicznych, zarówno podczas zatrudnienia, jak i po jego zakończeniu.
4. Zabrania się pracownikom:
   a) ujawniania danych osobowych zawartych w obsługiwanych systemach osobom nieuprawnionym.
   b) kopiowania baz danych lub ich części bez wyraźnego upoważnienia ADO danych.
   c) przetwarzania danych w sposób inny niż wynikający z obowiązujących przepisów prawa oraz wytycznych ADO.
5. Pracownicy mają obowiązek:
   a) wspierania ADO w realizacji zadań dotyczących ochrony danych osobowych, w tym wykonywania jego zaleceń,
   b) natychmiastowego powiadomienia ADO wszelkich nieprawidłowościach związanych z bezpieczeństwem przetwarzania danych osobowych, w tym o podejrzeniu naruszenia danych lub innych incydentach dotyczących ochrony danych,
   c) współpracy z IOD przy wykonywaniu czynności na danych osobowych.

6. Pracownicy, którzy nie wypełniają obowiązków wynikających z Polityki mogą być pociągnięci do odpowiedzialności za naruszenie obowiązków pracowniczych lub nienależyte wykonanie obowiązków. W szczególności dotyczy to sytuacji, w których pracownik nie poinformuje ADO lub IOD o wystąpieniu incydentu naruszenia ochrony danych osobowych.

§ 6

1. **Każdorazowo zapewnia się realizację praw osób fizycznych w związku z przetwarzaniem danych osobowych, poprzez:**
   a) **spełnianie obowiązku informacyjnego** - każdej osobie fizycznej, której dane dotyczą, należy przekazać informacje wymagane przy zbieraniu danych w co najmniej minimalnym zakresie wynikającym z art. 13 i 14 RODO. Należy zapewnić udokumentowanie realizacji tych obowiązków. Nie zbiera się podpisów osób fizycznych pod dokumentem potwierdzającym spełnienie obowiązku informacyjnego, jeżeli spełnienie tego obowiązku da się wykazać w inny sposób.
   b) **obsługa żądań** - każdej osobie fizycznej, której dane dotyczą, należy zapewnić możliwość żądania informacji i składania wniosków związanych z realizacją praw osób fizycznych w związku z przetwarzaniem danych osobowych. W szczególności ADO zapewnia odpowiednie kanały komunikacji takie jak e-mail, telefon, formularz kontaktowy tak, aby realizacja praw przebiegała w sposób jak najmniej uciążliwy dla osób fizycznych
   c) **informowanie o naruszeniach** - ADO wdraża procedury dotyczące zgłaszania naruszeń oraz informowania osób, których dane były przedmiotem naruszenia.

§ 7

1. Każda osoba realizująca proces związany z przetwarzaniem danych osobowych zobowiązana jest zaplanować go w sposób uwzględniający ochronę danych osobowych i spełnienie wymogów przetwarzania wynikających z RODO. W razie jakichkolwiek wątpliwości przy planowaniu danego procesu, należy skontaktować się z ADO lub IOD w celu właściwego zaprojektowania procesu (zasada **privacy as design**).
2. Każda osoba realizująca proces związany z przetwarzaniem danych osobowych zobowiązana jest zaplanować go taki sposób, aby w celu zapewnienia jak najszerszej ochrony danych osobowych osób fizycznych, nie było wymagane, aby ta osoba musiała podejmować jakiekolwiek czynności z własnej inicjatywy. W szczególności nie odbiera się od osób fizycznych żadnych dodatkowych oświadczeń, jeżeli nie jest to wymagane przepisami prawa. Należy jednoznacznie i wyraźnie informować osoby fizyczne, które oświadczenia są dobrowolne, a które obowiązkowe (zasada **privacy as default)**.

§ 8

ADO wdraża niezbędne środki i procedury mające na celu ochronę danych osobowych, zgodnie z obowiązującymi przepisami RODO i Ustawy. W ramach tych działań ADO realizuje poniższe obowiązki:

1. Przeprowadzanie analizy ryzyka. Zgodnie z art. 32 RODO, ADO dokonuje regularnej analizy ryzyka dotyczącego bezpieczeństwa przetwarzania danych osobowych, uwzględniając charakter, zakres, kontekst oraz cele przetwarzania. Ocena ryzyka obejmuje identyfikację potencjalnych zagrożeń oraz wdrożenie adekwatnych środków technicznych i organizacyjnych, mających na celu ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmianą, ujawnieniem lub dostępem do danych osobowych.
2. Ocena skutków dla ochrony danych. W przypadkach, gdzie przetwarzanie danych może wiązać się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, ADO przeprowadza ocenę skutków dla ochrony danych zgodnie z art. 35 RODO. Ocena taka jest obowiązkowa, gdy np. przetwarzanie obejmuje systematyczne i zautomatyzowane podejmowanie decyzji na podstawie danych osobowych, które wywołują skutki prawne wobec osoby, której dane dotyczą.
3. Zabezpieczenie fizyczne danych. Zgodnie z wymogami art. 32 ust. 1 lit. b RODO, ADO wdraża odpowiednie środki techniczne i organizacyjne, mające na celu ochronę pomieszczeń, w których przetwarzane są dane osobowe, przed nieuprawnionym dostępem. Ochrona ta obejmuje kontrolę dostępu, monitorowanie oraz systemy alarmowe.
4. Zarządzanie incydentami. W przypadku naruszenia ochrony danych osobowych, ADO działa zgodnie z art. 33 i 34 RODO, który nakłada obowiązek zgłoszenia incydentu do organu nadzorczego (w Polsce jest to Prezes Urzędu Ochrony Danych Osobowych - PUODO) w ciągu 72 godzin od momentu jego wykrycia, chyba że naruszenie nie stwarza ryzyka dla praw i wolności osób fizycznych. ADO jest również zobowiązany do poinformowania osób, których dane dotyczą, jeśli istnieje ryzyko dla ich praw.
5. Weryfikacja transgranicznego przetwarzania danych. ADO dokonuje analizy i identyfikacji procesów przetwarzania, w których może dochodzić do przekazywania danych osobowych poza Europejski Obszar Gospodarczy (EOG), zgodnie z art. 44–49 RODO. ADO zobowiązany jest do zapewnienia, że przekazywanie danych do państw trzecich odbywa się na podstawie odpowiednich gwarancji, takich jak decyzja o odpowiednim poziomie ochrony danych wydana przez Komisję Europejską lub stosowanie standardowych klauzul ochrony danych.
6. Automatyzacja procesów decyzyjnych. ADO identyfikuje procesy, w których podejmowane są decyzje wyłącznie w sposób zautomatyzowany, w tym profilowanie, zgodnie z art. 22 RODO.

W takim przypadku ADO zapewnia, że osoby, których dane dotyczą, mają prawo do sprzeciwu wobec takiego przetwarzania oraz do uzyskania interwencji człowieka, a także do wyrażenia własnego stanowiska.

§ 9

1. Rejestr pełni kluczową rolę w procesie zarządzania danymi osobowymi, będąc narzędziem wskazującym na procesy przetwarzania danych osobowych.
2. W Rejestrze każda czynność przetwarzania, którą ADO uznał za odrębną, powinna zawierać co najmniej następujące elementy:
   a) nazwa czynności przetwarzania – nazwa określająca, czego dotyczy dana czynność przetwarzania.
   b) cel przetwarzania – precyzyjny cel przetwarzania danych zgodny z art. 30 ust. 1 lit. b RODO.
   c) opis kategorii osób, których dane dotyczą – np. pacjenci, klienci, pracownicy, kontrahenci, zgodnie z art. 30 ust. 1 lit. c RODO.
   d) opis kategorii danych osobowych – wskazanie rodzaju przetwarzanych danych (np. dane identyfikacyjne, kontaktowe, dokumentacja medyczna), zgodnie z art. 30 ust. 1 lit. c RODO.
   e) podstawa prawna przetwarzania danych – określenie podstawy prawnej (np. zgoda, umowa, obowiązek prawny), a jeśli przetwarzanie opiera się na uzasadnionym interesie ADO, szczegółowe uzasadnienie tego interesu (art. 6 ust. 1 lit. f RODO).
   f) sposób zbierania danych – opis procesu pozyskiwania danych (np. bezpośrednio od osoby, której dane dotyczą, z formularzy internetowych).
   g) opis kategorii odbiorców danych – określenie, kto otrzymuje dane, w tym również przetwarzający działający na zlecenie ADO (art. 30 ust. 1 lit. d RODO).
   h) informacja o przekazaniu danych poza EU/EOG – szczegóły dotyczące przekazywania danych osobowych poza Europejski Obszar Gospodarczy oraz zastosowanych zabezpieczeń (art. 30 ust. 1 lit. e RODO).
   i) ogólny opis technicznych i organizacyjnych środków ochrony danych – opis zastosowanych środków bezpieczeństwa, zgodnie z art. 32 RODO.
3. ADO ma obowiązek prowadzenia Rejestru, który umożliwia inwentaryzację oraz monitorowanie sposobu przetwarzania danych osobowych w organizacji.
4. W celu utrzymania aktualności i kompletności Rejestru, ADO współpracuje z IOD w procesie jego uzupełniania i aktualizacji. Procedura ta obejmuje następujące kroki:
   a) ADO jest podmiotem inicjującym wprowadzanie danych do Rejestru.
   b) zgłaszanie nowych czynności przetwarzania – w przypadku rozpoczęcia nowych procesów przetwarzania danych osobowych, ADO niezwłocznie informuje IOD o rozpoczęciu takiego

przetwarzania. ADO dostarcza wszystkie niezbędne informacje dotyczące charakteru, celu oraz zakresu przetwarzania.

c) ocena i klasyfikacja – IOD, we współpracy z ADO, dokonuje oceny nowych czynności przetwarzania pod kątem ryzyka, zgodności z przepisami i wpisania ich do Rejestru. IOD wspiera również ADO w identyfikacji kategorii danych, podstaw prawnych przetwarzania oraz ewentualnych odbiorców danych.

d) aktualizacja istniejących wpisów – IOD jest odpowiedzialny za monitorowanie i weryfikację aktualności Rejestru. W przypadku zgłoszenia przez ADO zmian w procesach przetwarzania (np. zmiana celu, dodanie nowych kategorii danych), IOD aktualizuje odpowiednie wpisy.

e) regularna kontrola Rejestru – IOD, w porozumieniu z ADO, przeprowadza okresowe przeglądy Rejestru, aby upewnić się, że wszystkie procesy przetwarzania są w pełni zgodne z obowiązującymi przepisami oraz wewnętrznymi regulacjami ADO.

f) raportowanie – IOD, jako osoba odpowiedzialna za monitorowanie przestrzegania przepisów ochrony danych, okresowo raportuje ADO o stanie Rejestru, w tym o ewentualnych nieprawidłowościach lub obszarach wymagających dodatkowych środków ochrony.

5. Wzór rejestru stanowi załącznik 2 do niniejszej Polityki.

§ 10

1. ADO dokumentuje w Rejestrze podstawy prawne przetwarzania danych osobowych dla każdej czynności przetwarzania, zgodnie z wymogami art. 30 ust. 1 lit. a RODO. Podając ogólną podstawę prawną przetwarzania, ADO dodatkowo precyzuje tę podstawę w zależności od specyficznych potrzeb i charakteru przetwarzania, w zgodzie z zasadami przepisów art. 6 i 9 RODO. W związku z tym:

   a) na podstawie art. 6 ust. 1 lit. a RODO oraz, w przypadku szczególnych kategorii danych, art. 9 ust. 2 lit. a RODO, ADO musi uzyskać wyraźną zgodę osoby, której dane dotyczą, na przetwarzanie jej danych osobowych. Zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna.

   b) zgodnie z art. 6 ust. 1 lit. c RODO, ADO przetwarza dane, gdy istnieje obowiązek wynikający z przepisów prawa, np. w celu realizacji obowiązków wynikających z prawa podatkowego, prawa pracy lub innych przepisów. W przypadku szczególnych kategorii danych, przetwarzanie może być dopuszczalne na podstawie art. 9 ust. 2 lit. b RODO, jeżeli jest to niezbędne do wypełnienia obowiązków prawnych ADO w zakresie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej.

c) zgodnie z art. 6 ust. 1 lit. d RODO, ADO może przetwarzać dane w celu ochrony żywotnych interesów osoby, której dane dotyczą, np. w sytuacji ratowania życia lub zdrowia. Dla szczególnych kategorii danych (art. 9 ust. 2 lit. c RODO) przetwarzanie jest możliwe, gdy jest ono niezbędne do ochrony żywotnych interesów osoby fizycznej, która jest fizycznie lub prawnie niezdolna do wyrażenia zgody (np. w nagłych przypadkach medycznych).

d) przetwarzanie na podstawie uzasadnionego interesu ADO, zgodnie z art. 6 ust. 1 lit. f RODO, wymaga dokładnego określenia tego interesu. Może to obejmować np. działania w zakresie marketingu bezpośredniego, zapobieganie nadużyciom czy dochodzenie roszczeń. Jednakże, dla przetwarzania szczególnych kategorii danych osobowych, uzasadniony interes nie jest wystarczającą podstawą przetwarzania zgodnie z art. 9 RODO.

e) zadania publiczne/władza publiczna – Przetwarzanie danych w związku z wykonywaniem zadań publicznych lub władzy publicznej opiera się na art. 6 ust. 1 lit. e RODO, gdzie podstawą jest przepis prawa krajowego lub unijnego. Dla szczególnych kategorii danych, przetwarzanie może być oparte na art. 9 ust. 2 lit. g RODO, jeżeli jest niezbędne do realizacji ważnego interesu publicznego, np. w zakresie zdrowia publicznego lub badań naukowych.

2. Współpraca między ADO a IOD w zakresie ustalania podstawy przetwarzania danych obejmuje:

a) ustalenie podstawy przetwarzania - przed rozpoczęciem nowych procesów przetwarzania, ADO wspólnie z IOD dokonują analizy, aby określić właściwą podstawę przetwarzania, w szczególności dla przetwarzania danych szczególnych kategorii.

b) przegląd procesów przetwarzania: - IOD w porozumieniu z ADO przeprowadza regularne przeglądy procesów przetwarzania danych, aby upewnić się, że każda czynność ma prawidłowo określoną podstawę prawną, zgodnie z art. 6 i 9 RODO.

c) w razie zmian w przetwarzaniu danych, IOD informuje ADO o konieczności aktualizacji Rejestru zgodnie z art. 30 RODO. Kierownicy komórek organizacyjnych są zobowiązani do informowania IOD o wszelkich zmianach w podstawie prawnej przetwarzania.

§ 11

1. ADO przykłada dużą wagę do transparentności, zrozumiałości oraz klarowności komunikacji z osobami, których dane są przetwarzane. W każdym przypadku, gdy osoba, której dane dotyczą, wyraża wolę skorzystania z przysługujących jej praw na mocy RODO, ADO rozpatruje te wnioski indywidualnie, zapewniając jednocześnie zgodność z przepisami.
2. Osobom, których dane dotyczą każdorazowo należy udostępnić dane do kontaktu z IOD. IOD może przyjmować wnioski dotyczące realizacji praw osób których dane dotyczą. IOD niezwłocznie informuje ADO o wpłynięciu wniosku.

3. ADO niezwłocznie i bez zbędnej zwłoki realizuje prawa osób fizycznych w zakresie przetwarzania ich danych osobowych, zgodnie z przepisami art. 15-22 RODO. W szczególności obejmuje to:
   a) prawo dostępu do danych – osoba, której dane dotyczą, ma prawo uzyskać potwierdzenie, czy jej dane są przetwarzane, a jeśli tak, dostęp do tych danych oraz informacje o ich przetwarzaniu,
   b) prawo do sprostowania danych – każda osoba, której dane są przetwarzane, ma prawo do żądania sprostowania nieprawidłowych danych osobowych oraz uzupełnienia niekompletnych danych,
   c) prawo do usunięcia danych („prawo do bycia zapomnianym") – osoba, której dane dotyczą, może żądać usunięcia swoich danych osobowych w określonych sytuacjach, np. gdy dane nie są już potrzebne do celów, w których były zbierane, lub gdy wycofa zgodę, na podstawie której dane były przetwarzane,
   d) prawo do przenoszenia danych – osoba, której dane dotyczą, ma prawo do otrzymania danych osobowych, w powszechnie używanym formacie i prawo do ich przekazania innemu administratorowi bez przeszkód ze strony ADO.
   e) prawo do sprzeciwu wobec przetwarzania danych – osoba, której dane dotyczą, ma prawo wnieść sprzeciw wobec przetwarzania jej danych osobowych na podstawie uzasadnionego interesu ADO, w tym przetwarzania danych w celach marketingowych.
   f) ADO zapewnia dostępne i jasne mechanizmy umożliwiające osobom fizycznym korzystanie z przysługujących im praw. W tym celu:
      - na stronie internetowej publikowane są informacje dotyczące praw osób fizycznych oraz instrukcje, jak z nich skorzystać,
      - udostępniane są dane kontaktowe oraz wskazywane są dostępne metody komunikacji (np. formularze elektroniczne, kontakt telefoniczny), w tym wymagania dotyczące weryfikacji tożsamości wnioskodawcy.
      - ADO informuje o potencjalnych kosztach realizacji wniosków (zgodnie z przepisami RODO, pierwsze żądanie jest realizowane nieodpłatnie, ale za dodatkowe żądania mogą być pobierane opłaty w uzasadnionych przypadkach).
4. ADO jest zobowiązany do udzielenia odpowiedzi na żądanie osoby, której dane dotyczą, bez zbędnej zwłoki, a w każdym przypadku w ciągu miesiąca od otrzymania żądania, zgodnie z art. 12 ust. 3 RODO. Termin ten może zostać przedłużony o kolejne dwa miesiące, jeśli żądanie jest szczególnie skomplikowane lub jeśli występuje wiele żądań. W przypadku przedłużenia terminu ADO poinformuje osobę, której dane dotyczą, o przyczynach opóźnienia oraz o

planowanym terminie realizacji żądania. Odpowiedzi udziela się w formie, w jakiej została złożona lub w formie jaką wskaże osoba składająca żądanie.

5. ADO prowadzi szczegółową dokumentację dotyczącą realizacji obowiązków informacyjnych oraz obsługi wniosków osób fizycznych, w tym poprzez Rejestr realizacji żądań w którym dokumentowane są wszystkie żądania dotyczące dostępu do danych, ich sprostowania, usunięcia, przenoszenia czy sprzeciwu, a także informacje o sposobie i terminie ich realizacji. W rejestrze nie odnotowuje się żądania o dostęp do dokumentacji medycznej, dla których prowadzona jest odrębna ewidencja. Wzór rejestru stanowi załącznik nr 5 do Polityki.

§ 12

1. ADO stosuje odpowiednie procedury weryfikacji tożsamości osób składających żądania dotyczące swoich praw wynikających z RODO. Weryfikacja jest przeprowadzana tylko wtedy, gdy ADO ma wątpliwości co do tożsamości osoby składającej wniosek, aby zapobiec nieuprawnionemu dostępowi do danych osobowych.
2. W przypadku udzielania informacji przez telefon, ADO wdraża następujące kroki weryfikacyjne:
    - osoba składająca żądanie może zostać poproszona o podanie kluczowych informacji, które są wcześniej zarejestrowane w systemach ADO, takich jak: imię i nazwisko, adres zamieszkania lub inny zarejestrowany adres do kontaktu, numer telefonu, który był podany podczas wcześniejszych kontaktów, data urodzenia lub inny identyfikator personalny (np. podanie ostatnich czterech cyfr PESEL, jeśli jest przetwarzany),
    - w przypadku dalszych wątpliwości, pracownik może zadać dodatkowe pytania weryfikacyjne dotyczące wcześniejszych działań osoby, takich jak: data ostatniego kontaktu z TERPA, data ostatniej wizyty lub usługi z której korzystała dana osoba.
3. W przypadku, gdy żądanie jest składane drogą e-mailową, pracownik podejmuje dodatkowe kroki weryfikacyjne poprzez kontakt telefoniczny. Weryfikacja odbywa się na takich samych zasadach jak w przypadku zgłoszeń telefonicznych, a jej celem jest potwierdzenie tożsamości osoby, która złożyła żądanie. Ponadto:
    - pracownik analizuje treść żądania oraz porównuje adres e-mail z danymi zarejestrowanymi w systemie. Jeśli adres e-mail wzbudzi wątpliwości lub nie odpowiada danym z systemu, pracownik nawiązuje kontakt telefoniczny,
    - pracownik dzwoni na zarejestrowany numer telefonu osoby, której dane dotyczą, i stosuje procedury weryfikacyjne opisane w sekcji dotyczącej weryfikacji telefonicznej:
4. Każda osoba, która udziela informacji zwierającej dane osobowe zobowiązana jest stosować procedurę określoną w niniejszym paragrafie.

§ 13

1. ADO realizuje zasadę minimalizacji przetwarzania danych osobowych, zgodnie z wymogami art. 5 ust. 1 lit. c RODO, zapewniając, że przetwarzane dane są adekwatne, stosowne i ograniczone do niezbędnego minimum. Minimalizacja obejmuje trzy kluczowe obszary: zakres danych, dostęp do danych oraz czas ich przechowywania.
2. Pracownik dokonuje starannej weryfikacji pozyskiwanych danych osobowych, aby zapewnić ich adekwatność względem celów przetwarzania.
3. ADO zapewnia, że dostęp do danych osobowych mają wyłącznie osoby, które go potrzebują w związku z realizacją swoich obowiązków służbowych, poprzez wdrożenie następujących ograniczeń:
   a) ADO ogranicza dostęp do pomieszczeń, w których przetwarzane są dane osobowe, wyłącznie dla osób posiadających stosowne upoważnienia,
   b) uprawnienia do dostępu do danych są aktualizowane każdorazowo przy zmianach w składzie personelu, zmianach ról osób oraz przy zmianach podmiotów przetwarzających dane osobowe na zlecenie ADO,
   c) ADO dokonuje przeglądu i aktualizacji uprawnień dostępowych przynajmniej raz na rok, aby zapewnić zgodność z aktualnymi potrzebami przetwarzania danych.
4. ADO wprowadza mechanizmy kontroli cyklu życia danych osobowych, które umożliwiają usunięcie danych, gdy przestaną być potrzebne do realizacji celów, dla których zostały zebrane:
   a) Kontrola cyklu życia danych. ADO stosuje mechanizmy, które umożliwiają kontrolowanie przydatności danych na podstawie terminów wskazanych w Rejestrze.
   b) Usuwanie danych. Dane, które przestały być potrzebne do realizacji celów przetwarzania, są usuwane z systemów informatycznych oraz dokumentacji papierowej. Procedura ta obejmuje również dane przechowywane na nośnikach kopii zapasowych.
   c) Archiwizacja danych. Dane, których przechowywanie jest wymagane ze względów prawnych, mogą być archiwizowane. Procedury archiwizacji i tworzenia kopii zapasowych uwzględniają wymogi dotyczące kontroli cyklu życia danych, w tym terminowe usuwanie danych po zakończeniu okresu archiwizacji.
5. ADO zapewnia, że kopie zapasowe danych osobowych, przechowywane w celach archiwalnych objęte mechanizmami kontroli i usuwania danych zgodnie z polityką przechowywania danych oraz procedurami backupu. Przetwarzanie takich danych jest zgodne z zasadą minimalizacji i odbywa się wyłącznie w przypadku potrzeby przywrócenia danych.

§ 14

1. Pracownicy zobowiązani są do zgłaszania wszelkich naruszeń ochrony danych osobowych, w szczególności takich które mogą mieć wpływ na prawa i wolności osób fizycznych. Procedura

ta została opracowana w celu szybkiego reagowania na incydenty naruszeń i zapewnienia zgodności z przepisami ochrony danych.

2. Pracownik, który zauważy, podejrzewa lub dowie się o naruszeniu ochrony danych osobowych, ma obowiązek natychmiastowego zgłoszenia tego incydentu do ADO lub IOD. Zgłoszenie powinno być dokonane niezwłocznie, bez zbędnej zwłoki, najlepiej w ciągu kilku godzin od wykrycia incydentu.
3. Zgłoszenie powinno zawierać:
   a) opis naruszenia w tym okoliczności wykrycia naruszenia.
   b) datę i czas wykrycia naruszenia.
   c) rodzaj danych, których dotyczy naruszenie.
   d) potencjalną liczbę osób, których dane mogły zostać naruszone.
   e) informacje o krokach podjętych bezpośrednio po wykryciu incydentu (np. wyłączenie dostępu, zabezpieczenie danych).
4. Po otrzymaniu zgłoszenia naruszenia ADO i IOD współdziałania w celu dokonania następujących czynności:
   a) dokonują wstępnej analizy naruszenia w celu oceny jego charakteru, skali i potencjalnych skutków dla osób, których dane dotyczą.
   b) dokumentują incydent w specjalnym rejestrze naruszeń ochrony danych osobowych,
   c) przeprowadzają szczegółową ocenę, czy naruszenie może powodować ryzyko naruszenia praw i wolności osób fizycznych,
5. Zgodnie z art. 33 RODO, jeśli naruszenie danych osobowych powoduje ryzyko naruszenia praw i wolności osób fizycznych, ADO zobowiązany jest do zgłoszenia naruszenia Prezesa Urzędu Ochrony Danych Osobowych (PUODO) nie później niż 72 godziny po stwierdzeniu naruszenia. Zgłoszenie powinno zawierać:
   a) opis charakteru naruszenia, w tym kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę rekordów danych osobowych.
   b) imię i nazwisko oraz dane kontaktowe IOD lub innej osoby kontaktowej.
   c) opis możliwych konsekwencji naruszenia.
   d) opis środków podjętych lub proponowanych przez ADO w celu zaradzenia naruszeniu, w tym, jeśli to właściwe, środków minimalizujących jego negatywne skutki.
6. Jeśli zgłoszenie nie zostanie dokonane w ciągu 72 godzin, ADO musi dołączyć wyjaśnienie powodów opóźnienia. IOD wspiera ADO w sporządzeniu wyjaśnienia
7. Po zgłoszeniu naruszenia, pracownik ma obowiązek:
   a) współpracować z ADO i IOD w celu wyjaśnienia szczegółów naruszenia.

b) przestrzegać zaleceń ADO i IOD dotyczących postępowania w związku z naruszeniem, w tym ewentualnych działań naprawczych.
c) przekazywać wszelkie dodatkowe informacje, które mogą mieć znaczenie dla oceny incydentu i minimalizacji jego skutków.

8. Jeżeli naruszenie danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, ADO zobowiązany jest do powiadomienia osób, których dane dotyczą, zgodnie z art. 34 RODO. Powiadomienie to musi zawierać:
   a) charakter naruszenia.
   b) imię i nazwisko oraz dane kontaktowe osoby do kontaktu (np. IOD).
   c) możliwe konsekwencje naruszenia.
   d) środki, które zostały podjęte w celu zaradzenia naruszeniu i minimalizacji jego skutków.
9. ADO jest zobowiązany prowadzić Rejestr naruszeń ochrony danych osobowych, w którym odnotowywane są wszystkie incydenty związane z naruszeniem ochrony danych, bez względu na to, czy naruszenie zostało zgłoszone do organu nadzorczego. Rejestr ten musi zawierać szczegółowe informacje o każdym naruszeniu, w tym:
   a) datę zgłoszenia incydentu.
   b) charakter naruszenia.
   c) kategorie danych osobowych, których dotyczyło naruszenie.
   d) podjęte działania naprawcze i środki minimalizujące ryzyko.
10. Rejestr prowadzony jest we współpracy z IOD. IOD na każdorazowe żądanie ADO przedstawi informacje niezbędne do prawidłowego uzupełnienia rejestru. Wzór Rejestru incydentów stanowi załącznik nr 4.

§ 15

1. W przypadku, gdy ADO zleca przetwarzanie danych osobowych innemu podmiotowi (tzw. podmiotowi przetwarzającemu), ADO musi zapewnić, że przetwarzanie odbywa się zgodnie z przepisami RODO oraz innych obowiązujących aktów prawnych, w tym Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta w odniesieniu do dokumentacji medycznej. Poniżej opisana procedura dotyczy zarówno powierzania przetwarzania danych zwykłych, jak i szczególnych kategorii danych osobowych, w tym dokumentacji medycznej.
2. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 RODO, który określa wymogi wobec podmiotów przetwarzających. Powierzenie to może nastąpić wyłącznie na podstawie pisemnej umowy powierzenia przetwarzania danych, zawierającej co najmniej następujące elementy:
   a) zakres, cel i charakter przetwarzania:

- określenie rodzaju danych osobowych, które będą przetwarzane (np. dane medyczne, dane osobowe pacjentów, dane pracowników).
- ustalenie celu przetwarzania (np. przechowywanie danych, analiza, przetwarzanie danych w systemie informatycznym).
- zdefiniowanie czasu trwania przetwarzania oraz szczegółowego charakteru czynności przetwarzania.

b) zobowiązania podmiotu przetwarzającego:
- podmiot przetwarzający zobowiązuje się do przetwarzania danych wyłącznie na udokumentowane polecenie ADO.
- zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z RODO (art. 32 RODO).
- poufność przetwarzanych danych osobowych – obowiązek zapewnienia, że osoby mające dostęp do danych podpisały zobowiązania do zachowania poufności.

c) podpowierzenie przetwarzania danych:
- podmiot przetwarzający może powierzać przetwarzanie innym podmiotom wyłącznie za wyraźną zgodą ADO, z zachowaniem tych samych warunków, jakie wynikają z umowy powierzenia.

d) wsparcie ADO w realizacji praw osób, których dane dotyczą:
- podmiot przetwarzający zobowiązany jest wspierać ADO w realizacji obowiązków związanych z realizacją praw osób, których dane dotyczą (np. dostęp do danych, sprostowanie, usunięcie).

e) powiadomienie o naruszeniach:
- w przypadku naruszenia ochrony danych osobowych podmiot przetwarzający ma obowiązek niezwłocznie poinformować ADO, aby umożliwić zgłoszenie naruszenia do organu nadzorczego (art. 33 RODO).

f) usuwanie lub zwrot danych:
- po zakończeniu przetwarzania danych osobowych, podmiot przetwarzający zobowiązany jest do usunięcia lub zwrotu wszystkich danych osobowych zgodnie z wytycznymi ADO, chyba że przepisy prawa wymagają dłuższego okresu przechowywania danych.

3. Powierzenie przetwarzania danych medycznych, w tym dokumentacji medycznej, podlega szczególnym wymogom wynikającym zarówno z RODO, jak i Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (art. 24, 26 i 30). Powierzając dokumentację medyczną należy zapewnić, że realizacja umowy nie nie spowoduje zakłóceń udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do

danych zawartych w dokumentacji medycznej. Należy również zobowiązać podmiot do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją tej umowy, także po śmierci pacjenta.

4. W przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej ADO.
5. Powierzenie danych osobowych jest ewidencjonowane w rejestrze. Wzór rejestru stanowi złącznik nr 10.

§ 16

Instrukcja zarządzania systemem informatycznym stanowi załącznik nr 2 do Polityki.

§ 17

1. Wszelkie zasady opisane w niniejszej Polityce Bezpieczeństwa są ściśle przestrzegane przez osoby upoważnione do przetwarzania danych osobowych. W szczególności osoby te zobowiązane są do działania z poszanowaniem dobra osób, których dane są przetwarzane, zgodnie z wymogami RODO oraz innymi obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych.
2. Zasady stosowania monitoringu wizyjnego w TERPA zostały ustanowione w odrębnym Regulaminie.
3. Dokument obowiązuje od dnia podania do wiadomości pracownikom TERPA.
4. Wszelkie istotne zmiany w niniejszej Polityce Bezpieczeństwa powinny być niezwłocznie ujawnione przez ADO oraz wdrożone w sposób zapewniający ich skuteczność i zgodność z aktualnymi przepisami prawa. ADO zapewnia, że pracownicy oraz współpracownicy zostaną poinformowani o wszelkich zmianach, a wdrożenie nowych zasad będzie odpowiednio nadzorowane.

Załączniki:

1. Instrukcja zarządzania systemem informatycznym.
2. Rejestr Czynności Przetwarzania Danych.
3. Rejestr upoważnień do przetwarzania danych osobowych.
4. Rejestr incydentów.
5. Rejestr Realizacji Żądań jednostki.

6. Wzór upoważnienia do przetwarzania danych osobowych.
7. Wzór odwołania upoważnienia do przetwarzania danych osobowych.
8. Wzór oświadczenia o przetwarzaniu danych osobowych zgodnie z RODO.
9. Analiza ryzyka
10. Rejestr powierzenia