# ZASADY I SPOSÓB PRZETWARZANIA DANYCH OSOBOWYCH ORAZ ICH ZABEZPIECZENIA W KZP

**ADO lub Administrator** (Administrator Danych Osobowych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jest nim **KZP przy Katowickich Wodociągach S.A., którą reprezentuje Zarząd KZP** ;

**Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, której dane dotyczą;

**Dane wrażliwe** oznaczają szczególną kategorię danych osobowych: stan zdrowia, dane karne w rozumieniu art.10 RODO – członków Zarządu lub Komisji rewizyjnej;

**Dane specjalne** oznaczają 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, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

**Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących oraz czynów zabronionych;

**Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

## 1 FILARY SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM DANYCH OSOBOWYCH W KZP

### 1.1 Legalność

**1.** ADO dba o ochronę prywatności i przetwarza dane na podstawie prawa i zgodnie z prawem.

**2.** Wyrazem legalności działań ADO jest także stosowanie się do zasad przetwarzania danych osobowych, opisanych w części pn. „Zasady ogólne przetwarzania danych osobowych”.

### 1.2 Bezpieczeństwo

**1.** ADO zapewnia odpowiedni poziom bezpieczeństwa danych, w tym ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych przetwarzanych w Jednostce, podejmując systematyczne działania w tym zakresie.

2. Działania modelujące bezpieczeństwo danych osobowych zostały opisane w dalszej części pn. „Bezpieczeństwo danych osobowych – przyjęte rozwiązania”.

### 1.3 Prawa podmiotu danych

1. ADO umożliwia osobom fizycznym, których dane przetwarza (tzw. podmiotom danych), egzekwowanie przysługujących im praw i prawa te realizuje.

### 1.4 Rozliczalność

1. ADO dokumentuje sposób w jaki spełnia obowiązki, aby w każdej chwili móc wykazać zgodność przetwarzania danych osobowych z prawem i rozliczalność.

2. Rozliczalność ma swoje odzwierciedlenie w realizacji i egzekwowaniu przyjętych zasad i procedur.

## 2 ZASADY OGÓLNE PRZETWARZANIA DANYCH OSOBOWYCH

Mając na względzie odpowiednie funkcjonowanie systemu zarządzania bezpieczeństwem danych osobowych, ADO przetwarza dane osobowe z poszanowaniem następujących **zasad ogólnych**:

### 2.1 Legalizm

1. Dane osobowe przetwarza się w oparciu o podstawę prawną i zgodnie z prawem.

2. ADO identyfikuje i weryfikuje podstawy prawne przetwarzania danych osobowych.

### 2.2 Rzetelność

1. Dane osobowe przetwarza się rzetelnie, z należytą starannością i uczciwie.

### 2.3 Transparentność (przejrzystość)

1. Dane osobowe przetwarza się w sposób przejrzysty z punktu widzenia osoby, której dane osobowe są przetwarzane.

### 2.4 Ograniczenie celu

1. Dane osobowe przetwarza się w konkretnych, wyraźnych i prawnie uzasadnionych celach.

### 2.5 Minimalizacja danych

1. ADO przetwarza dane osobowe adekwatne, stosowne oraz ograniczone do zakresu niezbędnego z punktu widzenia celów, dla których są przetwarzane.

**2.** ADO posiada zasady i metody *zarządzania minimalizacją przetwarzania danych osobowych,* a w tym:

#### 2.5.1 Minimalizacja zakresu

**1)** ADO weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania

**2)** ADO dokonuje okresowego corocznego przeglądu przetwarzanych danych i zakresu ich przetwarzania, w tym inwentaryzacji danych osobowych.

**3)** ADO uwzględnia zasady ochrony danych osobowych począwszy od etapu projektowania systemów lub planowania czynności przetwarzania danych osobowych (*privacy by design*).

#### 2.5.2 Minimalizacja dostępu

**1)** ADO stosuje ograniczenia dostępu do danych osobowych: ***prawne*** (*zobowiązania do poufności, zakresy upoważnień*), ***logiczne*** (*ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe*).

**2)** ADO dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

**3)** ADO dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich.

#### 2.5.3 Minimalizacja czasu

**1)** ADO usuwa dane osobowe, których zakres przydatności ulega ograniczeniu wraz z upływem czasu. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez ADO.

**2)** Wszelką dokumentację zawierającą dane osoby, po upływie jej przydatności ADO niszczy przy użyciu niszczarek.

### 2.6 Prawidłowość

**1.** Przetwarza się dane osobowe prawidłowe i w razie potrzeby uaktualniane.

**2.** Podejmuje się wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

### 2.7 Ograniczanie przechowywania

**1.** Dane osobowe przechowywane są w formie umożliwiającej identyfikację osoby, której dotyczą przez okres nie dłuższy, niż jest to niezbędne do osiągnięcia celów, w których dane te są przetwarzane.

**2.** Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki

techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą.

### 2.8 Dostępność, Integralność i Poufność

1. Dane osobowe przetwarza się w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed przypadkowym lub niezgodnym z prawem
   a. zniszczeniem lub utratą – zachowanie **dostępności** danych,
   b. modyfikacją – zachowanie **integralności** danych,
   c. nieuprawnionym ujawnieniem lub nieuprawnionym dostępem – zachowanie **poufności** danych.
2. Bezpieczeństwo realizuje się za pomocą odpowiednich środków technicznych lub organizacyjnych, opisanych w odpowiednich zasadach i procedurach funkcjonujących u ADO.

## 3 BEZPIECZEŃSTWO DANYCH OSOBOWYCH – PRZYJĘTE ROZWIĄZANIA

ADO zapewnia odpowiedni poziom bezpieczeństwa danych osobowych poprzez następujące działania:

### 3.1 Dokumentacja bezpieczeństwa

1. ADO opracował i zatwierdził, opublikował i zakomunikował wszystkim pracownikom i członkom KZP *Zasady i sposób przetwarzania danych osobowych oraz ich zabezpieczenia w KZP.* Jest to niniejszy dokument.
2. ADO poddaje „Zasady i sposób przetwarzania danych osobowych oraz ich zabezpieczenia w KZP" regularnym przeglądom i aktualizacji, jeśli zajdzie taka potrzeba.
3. ADO przechowuje i udostępnia zainteresowanym podmiotom oryginalne i aktualnie obowiązujące „Zasady i sposób przetwarzania danych osobowych oraz ich zabezpieczenia w KZP".
4. ADO nie ujawnia i nie udostępnia informacji, które wpłynęłyby na osłabienie bezpieczeństwa danych osobowych w KZP.

### 3.2 Organizacja bezpieczeństwa

1. Wiodące obowiązki w zakresie ochrony danych osobowych, są realizowane przez:

   **Administratora Danych Osobowych (ADO)** – **Zarząd KZP**– odpowiada za funkcjonowanie systemu zarządzania bezpieczeństwem danych osobowych;

2. ADO nie zatrudnia pracowników.

### 3.3 Zarządzanie danymi osobowymi

#### 3.3.1 Inwentaryzacja i retencja danych

1) ADO dokonuje **identyfikacji (inwentaryzacji) zasobów danych osobowych** w Jednostce, w tym zbiorów danych osobowych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, sprzętu, narzędzi informatycznych, w szczególności:
   - przypadków przetwarzania **danych wrażliwych** (szczególna kategoria danych osobowych: stan zdrowia, dane karne w rozumieniu art.10 RODO – członków Zarządu lub Komisji rewizyjnej danych specjalnych oraz danych karnych);
   - przypadków przetwarzania danych osób, których Jednostka nie identyfikuje (**dane niezidentyfikowane**);
   - **profilowania**;
   - **współadministrowania** danymi.
2) W stosunku do zidentyfikowanych zbiorów danych osobowych, ADO wskazuje odpowiedzialność za te dane.
3) ADO opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych (RCPD) w Jednostce. RCPD jest narzędziem ewidencji zasobów danych osobowych oraz procesów przetwarzania danych osobowych, jak również rozliczania zgodności z ochroną danych w Jednostce.

## 3.4 Bezpieczeństwo oparte na analizie ryzyka

### 3.4.1 Poziom ryzyka i racjonalność bezpieczeństwa

1) Poziom stosowanego bezpieczeństwa danych osobowych uzależnia się od **oszacowanego poziomu ryzyka**.
2) Środki i mechanizmy ochrony danych osobowych stosuje się z zachowaniem zasady **racjonalności** (zdrowego rozsądku), uwzględniając przy tym konieczność zapewnienia *adekwatności, skuteczności i efektywności* mechanizmów kontroli zarządczej w kontekście ryzyka naruszenia praw i wolności osób fizycznych, których dane są przetwarzane.
3) **Przynajmniej raz w roku** ADO przeprowadza **analizę ryzyka** dla czynności przetwarzania danych osobowych, której celem jest weryfikacja zastosowanych zabezpieczeń pod względem ich racjonalności i przydatności w stosunku do zmieniających się zagrożeń.
4) W przypadkach określonych przepisami RODO oraz, gdy w wyniku analizy ryzyka oszacowany zostanie **wysoki poziom ryzyka**, ADO przeprowadza ocenę skutków dla ochrony danych (DPIA).

### 3.4.2 Organizacyjne i techniczne wymogi i środki ochrony

1) Określenie **organizacyjnych i technicznych wymogów i środków bezpieczeństwa** przetwarzania danych osobowych zawarto w Rejestrze czynności przetwarzania danych osobowych.

## 3.5 Kontrola dostępu do danych osobowych

### 3.5.1 Upoważnienia

1) Do przetwarzania danych osobowych w Jednostce dopuszczone są wyłącznie upoważnione przez ADO osoby fizyczne.
2) Wszystkie osoby upoważnione do przetwarzania danych osobowych zobowiązane są do:
    1) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami;
    2) postępowania zgodnie z ustaloną przez ADO niniejszymi „Zasadami i sposobem przetwarzania danych osobowych oraz ich zabezpieczeniem w KZP";
    3) stosowania się do wydawanych przez ADO procedur, wytycznych oraz poleceń służbowych w zakresie ochrony danych osobowych;
    4) ścisłego przestrzegania zakresu udzielonego upoważnienia do przetwarzania danych osobowych w ramach wykonywania powierzonych tej osobie obowiązków oraz wykonywania ich wyłącznie na polecenie ADO lub osoby przez niego upoważnionej;
    5) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, także po ustaniu stosunku prawnego łączącego osobę upoważnioną z ADO lub odwołaniu tej osoby z funkcji pełnionej u ADO;
    6) korzystania z narzędzi informatycznych, w tym oprogramowania, urządzeń oraz nośników w sposób zgodny z obowiązującą procedurą oraz wskazaniami ADO
    7) zabezpieczania danych osobowych przed ich utratą, nieautoryzowaną zmianą lub ujawnieniem osobom nieupoważnionym;
    8) zgłaszania niewłaściwego funkcjonowania systemu zarządzania bezpieczeństwem danych osobowych do ADO,
    9) informowania ADO o przypadkach naruszenia bezpieczeństwa danych osobowych.

### 3.5.2 Dostęp do systemów i aplikacji informatycznych

Dostęp do danych osobowych przetwarzanych z wykorzystaniem systemów i aplikacji informatycznych możliwy jest na podstawie upoważnienia wydawanego przez ADO.

## 3.6 Obszary przetwarzania danych osobowych

1) Obszarem przetwarzania danych jest obszar, w którym wykonywana jest choćby jedna z operacji przetwarzania danych osobowych (patrz definicja przetwarzania).
2) Należy chronić dane osobowe przed wszelkim dostępem do nich osób nieupoważnionych.
3) Nośników informacji w formie papierowej zawierających przetwarzane przez ADO dane osobowe, nie można pozostawiać w miejscach ogólnodostępnych i niezabezpieczonych, jak również nie wolno udostępniać osobom nieupoważnionym.

**4)** Pomieszczenia, w których są przetwarzane przez ADO dane osobowe muszą być zamykane na klucz bądź powinny być wyposażone w innego rodzaju system umożliwiający blokadę wejścia do takiego pomieszczenia.

**5)** Pomieszczenia, do których dostęp mają też osoby nieupoważnione są zamykane na klucz, który jest pobierany na portierni i potwierdzany wpisem w Ewidencji Pobrań Kluczy.

**6)** Miejsca (np. szafy, szafki) przeznaczone do przechowywania przetwarzanych przez ADO danych osobowych muszą być zamykane na klucz lub powinny być wyposażone w innego rodzaju system umożliwiający blokadę otwarcia takich miejsc.

**7)** Klucze do tych miejsc są przechowywane w specjalnej skrzynce na klucze z kodem dostępu, który znają wyłącznie osoby upoważnione przez ADO do przetwarzania danych osobowych, w zakresie zgodnym z zakresem upoważnienia do przetwarzania danych osobowych.

**8)** Miejsca z danymi osobowymi są otwarte tylko na czas potrzebny na dostęp do tych danych, a następnie zostają zamknięte.

**9)** Pomieszczenia, w których znajdują się dane osobowe przetwarzane przez ADO pozostają zawsze pod bezpośrednim nadzorem. Opuszczenie pomieszczenia, w których znajdują się dane osobowe przetwarzane przez ADO musi być poprzedzone przeniesieniem dokumentów zawierających dane osobowe do odpowiednio zabezpieczonego miejsca (np. szafy, szafki).

**10)** Dokumentacji, która zawiera zbiory danych osobowych, nie można wynosić poza teren KZP.

**11)** Dane chronione w formie papierowej mogą znajdować się w miejscach ogólnodostępnych (np. na biurku) tylko i wyłącznie w trakcie wykonywania czynności służbowych związanych z przetwarzaniem danych osobowych, a następnie muszą być przeniesione i przechowywane w miejscach przeznaczonych do tego celu (np. w zamykanej na klucz szafie lub szafce).

**12)** Wydruki robocze, które zawierają dane osobowe błędne lub zdezaktualizowane muszą być niezwłocznie trwale zniszczone przy użyciu niszczarki do papieru lub w inny sposób, zapewniający skuteczne ich usunięcie lub pseudonimizację danych osobowych.

**13)** Zabrania się:

**a) przetwarzania danych osobowych poza obszarem przetwarzania**, który stanowi siedziba KZP

**b) wyrzucania dokumentów** zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,

**c) pozostawiania dokumentów**, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,

**d) pozostawiania dokumentów na biurku po zakończonej pracy,** pozostawiania otwartych dokumentów na ekranie monitora bez blokady komputera,

**e) pozostawiania kluczy** w drzwiach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,

**f) pozostawiania bez nadzoru osób postronnych** przebywających w pomieszczeniach KZP, w których przetwarzane są dane osobowe,

**g) ignorowania nieznanych osób** z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,

**h)** przekazywania danych osobowych **osobom nieupoważnionym**.

### 3.7 Udostępnianie danych (kontakty z osobami i podmiotami spoza KZP)

1. ADO udostępnia dane osobowe innym podmiotom na podstawie przepisów prawa oraz „Zasad i sposobu przetwarzania danych osobowych oraz ich zabezpieczenia w KZP” .
2. W przypadku udostępniania danych osobowych podmiotom zewnętrznym (odbiorcom) odnotowuje się ten fakt w Rejestrze udostępnień.
3. **Zabrania się** udzielania jakichkolwiek informacji zawierających dane osobowe osobom i podmiotom nieuprawnionym.
4. Udostępnianie danych osobowych odbywa po uprzedniej **weryfikacji tożsamości** osoby wnioskującej o udostepnienie.
5. **Celem weryfikacji tożsamości** jest dążenie do potwierdzenia, że osoba zwracająca się udostępnienie danych osobowych jest tą, za którą się podaje i ma prawo uzyskać dostęp do danych osobowych.
6. W przypadku wątpliwości lub trudności w potwierdzeniu tożsamości, **nie udostępnia danych osobowych** zanim nie zostanie przeprowadzona skuteczna weryfikacja tożsamości w oparciu o **uznane dane weryfikujące**,
7. Zakres udostępnianych danych osobowych **nie może być szerszy, niż jest to niezbędne** do właściwej realizacji zadań nałożonych przepisami prawa.

#### 3.7.1 Kontakty z organami i instytucjami publicznymi

1) W przypadku udostępniania danych osobowych organom i instytucjom publicznym, odbywa się to na podstawie obowiązujących przepisów prawa.
2) Udostępnianie danych osobowych **podczas rozmowy telefonicznej** możliwe jest tylko w przypadku, gdy wykonuje się lub odbiera połączenie z numerem telefonu, który uwiarygadnia tożsamość odbiorcy danych osobowych. W przeciwnym razie, koniecznym jest dokonanie **weryfikacji tożsamości** w oparciu o opisane wyżej zasady.

#### 3.7.2 Sytuacje kryzysowe i nagłe

1) Udostępnianie danych osobowych w **sytuacjach nagłych lub kryzysowych wymaga weryfikacji tożsamości** odbiorcy danych, chyba, że mogłoby to spowodować znaczne utrudnienie w prowadzeniu akcji ratunkowej lub pomocowej. Koniecznym jest wykazanie ostrożności w kwestii tego komu udostępnia się dane osobowe.
2) Powyższe należy rozpatrywać w szczególności w sytuacjach, w których udostępnienie danych osobowych jest niezbędne dla **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) Należy udostępniać dane osobowe **tylko w takim zakresie**, który niezbędny jest w kontekście zaistniałej sytuacji nagłej lub kryzysowej.

#### 3.7.3 Kontakty z zewnętrznymi usługodawcami (powierzenie przetwarzania)

1) W przypadkach dostępu podmiotów zewnętrznych do danych osobowych dla celów realizacji usług na rzecz KZP lub wynikających z realizowanych przez Jednostkę zadań, które wiążą się z przetwarzaniem danych osobowych, zawiera się stosowną **umowę powierzenia przetwarzania**.

2) Umowa powierzenia przetwarzania zawiera w szczególności:

   **a.** Przedmiot i czas trwania przetwarzania,
   **b.** Charakter i cel przetwarzania
   **c.** Rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
   **d.** Obowiązki i prawa ADO.

3) Umowa określa wymagania bezpieczeństwa, których celem jest minimalizacja ryzyka wynikającego z dostępu podmiotu zewnętrznego do aktywów KZP w tym w szczególności do danych osobowych.

#### 3.7.4 Anonimizacja

1) Informacje przekazywane podmiotom zewnętrznym do celów statystycznych, badawczych, itp., mogą zostać udostępnione jedynie za **wyraźną zgodą ADO**, po uprzednim ich zanonimizowaniu (usunięciu elementów, które pozwalają na identyfikowanie tożsamości).

### 3.8 Incydenty i naruszenie bezpieczeństwa

1. Zdarzenia związane z bezpieczeństwem danych osobowych należy zgłaszać **tak szybko, jak to jest możliwe.**
2. W celu zgłoszenia należy się kontaktować **z ADO.**
3. Obowiązkowemu zgłoszeniu i rejestracji podlegają również wszelkie zaobserwowane i podejrzewane **słabości** związane z bezpieczeństwem przetwarzania danych osobowych.

### 3.9 Sprawdzanie zgodności

1. ADO zapewnia realizację czynności mających na celu **sprawdzenie zgodności** obowiązujących „Zasad i sposobu przetwarzania danych osobowych oraz ich zabezpieczenia w KZP”, wraz z procedurami, oraz zgodności przetwarzania danych osobowych z obowiązującymi przepisami w zakresie ochrony danych osobowych, w tym w szczególności z RODO, UODO oraz innymi przepisami sektorowymi;

# 4 OBSŁUGA PRAW OSOBY, KTÓREJ DANE SĄ PRZETWARZANE (PODMIOT DANYCH)

ADO spełnia obowiązki informacyjne względem podmiotów danych, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

## 4.1 Realizacja praw osoby, której dane osobowe są przetwarzane.

1. ADO przekazuje prawem wymagane informacje przy zbieraniu danych osobowych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
2. ADO weryfikuje i zapewnia możliwość efektywnego wykonania przez siebie i swoich przetwarzających każdego typu żądania podmiotów danych.
3. ADO zapewnia odpowiednie nakłady i procedury, aby żądania podmiotów danych były realizowane w terminach i w sposób wymagany przez RODO i udokumentowane.
4. ADO stosuje procedury pozwalające na ustalenie konieczności zawiadomienia podmiotów danych dotkniętych zidentyfikowanym naruszeniem ochrony danych.

## 4.2 Privacy by design – ochrona danych osobowych na etapie projektowania.

1. Przy wprowadzaniu zmian, uruchamianiu nowych projektów i inwestycji w Jednostce ADO ocenia wpływ planowanej zmiany na ochronę danych, zapewnienie prywatności (w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji przetwarzania).

# 5.EKSPORT DANYCH OSOBOWYCH DO PAŃSTW TRZECICH ALBO DO ORGANIZACJI MIĘDZYNARODOWYCH

ADO posiada zasady weryfikacji, czy Jednostka nie przekazuje danych do państw trzecich (tzn. poza UE i poza obszar EOG) albo do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, gdy ma ono miejsce.

# 6. OBOWIĄZKI INFORMACYJNE

1. ADO spełnia obowiązki informacyjne względem osób, których dane przetwarza, jak też zapewnia realizację przysługujących im uprawnień, realizując otrzymane w tym zakresie żądania, w tym:
   **a)** obowiązków informacyjnych;
   **b)** realizacji praw osób fizycznych.
2. ADO weryfikuje pod kątem celów przetwarzania danych osobowych stosowane klauzule informacyjne, jak też identyfikuje potrzebę ich wprowadzenia w zakresie spełnienia obowiązków informacyjnych wobec osób, których dane dotyczą,

zgodnie z art. 13 RODO i art. 14 RODO. ADO zapewnia, żeby stosowane klauzule informacyjne sformułowane były w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności, gdy informacje są kierowane do dziecka. Pracownicy ADO Przetwarzający Dane są zobowiązani konsultować z Zarządem Jednostki potrzebę zastosowania klauzul informacyjnych, ich treść oraz zgodność z prawem.

**3.** Zarząd Jednostki stosownie do art. 23 RODO, sprawdzają, czy prawo Unii lub prawo państwa członkowskiego, któremu podlega ADO, nie zawiera ograniczeń w zakresie wykonywania obowiązków informacyjnych.

**4.** W przypadku zbierania przez ADO danych od osoby, której dane dotyczą, ADO informuje taką osobę podczas pozyskiwania danych osobowych oraz w innych sytuacjach, jak też zapewnia, by realizacja tych obowiązków została udokumentowana.

**5.** ADO wywiązuje się z prawnych terminów realizacji obowiązków informacyjnych względem osób fizycznych.

**6.** ADO zapewnia czytelność i odpowiednią formę przekazywanych informacji oraz komunikacji z osobami, których dane przetwarza.

**7.** ADO informuje osobę fizyczną, której dane dotyczą o planowanej zmianie celu przetwarzania.

**8.** ADO informuje osobę fizyczną, której dane dotyczą przed uchyleniem ograniczenia przetwarzania danych.

**9.** ADO informuje Odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

**10.** ADO informuje osobę fizyczną, której dane dotyczą, o prawie wniesienia sprzeciwu wobec przetwarzania dotyczących jej danych, najpóźniej przy pierwszym kontakcie z tą osobą.

**11.** ADO informuje osobę fizyczną, której dane dotyczą o przedłużeniu terminu miesięcznego do rozpatrzenia żądania (wniosku/sprzeciwu) na rozpatrzenie żądania (wniosku/sprzeciwu) tej osoby. ADO bez zbędnej zwłoki zawiadamia osobę fizyczną o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

**12.** ADO określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

**13.** ADO prowadzi dokumentację w zakresie obowiązków informacyjnych, zawiadomień oraz żądań osób fizycznych, których dotyczą dane.

## 7. JEDNOSTKA JAKO WSPÓŁADMINISTRATOR

**1.** ADO weryfikuje, czy nie występuje w relacji współadministrowania z innym podmiotem.

**2.** Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 RODO i art. 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą(art.26 ust. 1 RODO).

**3.** Uzgodnienia, o których mowa w art. 26 ust. 1 RODO, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

**4.** Niezależnie od uzgodnień, o których mowa w art. 26 ust. 1 RODO, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego z administratorów.

**5.** KZP jako współadministrator wdraża i stosuje niniejsze „Zasady i sposób przetwarzania danych osobowych oraz ich zabezpieczenia w KZP", by przetwarzanie odbywało się zgodnie z RODO i aby mógł wykazać zgodność przetwarzania danych osobowych z RODO.

## 8. POSTANOWIENIA KOŃCOWE

**1.** W sprawach nieuregulowanych w niniejszych „Zasadach i sposobach przetwarzania danych osobowych oraz ich zabezpieczeniach w KZP" zastosowanie znajdują przepisy RODO oraz UODO.