POLITYKA OCHRONY DANYCH OSOBOWYCH

Podpis Administratora:

Dariusz Witczak
Dyrektor Miejsko-Gminnego Zespołu Oświaty w Janikowie

Spis treści

Rozdział I
Przepisy Ogólne

Art. 1. Informacje wstępne

1. Polityka ochrony danych osobowych zwana dalej „Polityką” jest dokumentem wewnętrznym Miejsko-Gminnego Zespołu Oświaty w Janikowie zwanego/zwanej* dalej również „Jednostką”, opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań wynikających z:

1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1, sprost.: Dz. Urz. UE L 127 z 23.05.2018, s. 2);
2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781 ze. zm.);
3) rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773);
4) przepisów szczególnych, regulujących funkcjonowanie Jednostki i przetwarzanych w ramach jej działalności danych osobowych;
5) dobrych praktyk z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych.

Art. 2. Zakres stosowania Polityki

1. Polityka ma zastosowanie do danych osobowych przetwarzanych przez Jednostkę w systemach informatycznych (sposób zautomatyzowany) oraz w postaci papierowej (sposób niezautomatyzowany).
2. Polityka ma także zastosowanie do danych osobowych przetwarzanych przez Jednostkę w ramach pracy zdalnej, której warunki szczegółowo określa **załącznik nr 19** do Polityki „Procedura ochrony danych osobowych przy pracy zdalnej”.
3. Środki techniczne i organizacyjne ujęte w Polityce mają również zastosowanie do danych osobowych przetwarzanych w projektach finansowanych ze środków zewnętrznych, chyba że umowa projektowa stanowi inaczej.

Art. 3. Deklaracja stosowania

1. Administratorzy ustanawiają Politykę oraz deklarują:
   1) podejmowanie wszystkich działań niezbędnych dla zapewnienia legalności

przetwarzanych danych;

2) stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane w zakresie problematyki bezpieczeństwa tychże danych;
3) stosowanie adekwatnych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym;
4) dążenie do zapewnienia poufności, dostępności oraz integralności danych osobowych.

Art. 4. Definicje

1. **Administrator** – Miejsko-Gminny Zespół Oświaty reprezentowany przez Dyrektora oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
2. **Aktywa** – wszelkie elementy posiadające wartość dla Jednostki (zasoby ludzkie, finansowe, informacyjne, organizacyjne, technologiczne, i fizyczne) mogące służyć do przetwarzania danych osobowych.
3. **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.
4. **Dane osobowe zwykłe** – wszelkie dane osobowe nienależące do szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, jak również danych dotyczących wyroków skazujących lub czynów zabronionych.
5. **Szczególne kategorie danych osobowych** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej) ujawniające informacje o stanie jej zdrowia; dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne

(przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej) oraz dane dotyczące seksualności lub orientacji seksualnej osoby fizycznej.

6. **Dane dotyczące wyroków skazujących i czynów zabronionych** – dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, które można przetwarzać wyłącznie pod nadzorem władz publicznych lub gdy pozwalają na to przepisy prawa krajowego lub prawa unijnego.
7. **Inspektor Ochrony Danych /IOD/ –** osoba wyznaczona przez Administratora lub Podmiot przetwarzający, posiadająca odpowiednie kwalifikacje zawodowe (wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych) oraz umiejętności wymagane do wypełniania zadań związanych z ochroną danych, zwana w treści Polityki również jako „IOD".
8. **Kopia zapasowa** – kopia danych lub oprogramowania, której celem wykonania jest odtworzenie systemu po awarii.
9. **Jednostka –** Miejsko-Gminny Zespół Oświaty w Janikowie.
10. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
11. **Administrator Systemów Informatycznych-** osoba lub podmiot wyznaczony przez Administratora do realizacji zadań w zakresie zarządzania, bieżącego nadzoru nad systemami informatycznymi oraz serwisu sprzętu komputerowego w Jednostce.
12. **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
13. **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

14. **Podatność -** słabość aktywu (zasobu) lub zabezpieczenia, które może być wykorzystane przez jedno lub więcej zagrożeń.
15. **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
16. **Polityka** – niniejsza Polityka ochrony danych osobowych.
17. **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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.
18. **Rejestr czynności przetwarzania danych osobowych –** rejestr czynności przetwarzania danych osobowych, o którym stanowi art. 30 ust. 1 RODO.
19. **Rejestr wszystkich kategorii czynności przetwarzania** – rejestr wszystkich kategorii czynności przetwarzania, o którym stanowi art. 30 ust. 2 RODO.
20. **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).
21. **Ryzyko** – potencjalna sytuacja, w której określone zagrożenie wykorzystując podatność aktywów lub grupy aktywów powodować może chociażby potencjalną szkodę majątkową lub niemajątkową dla Jednostki.
22. **System informatyczny** – system przetwarzania danych, w tym danych osobowych, łącznie z zasobami technicznymi (stanowisko pracy, jednostka centralna, system zarządzania, sieć teletransmisyjna), pracownikami oraz określonym obszarem działania (pomieszczeniami).
23. **Moduł systemu informatycznego-** dedykowana część systemu informatycznego przetwarzającego dane osobowe.
24. **Szacowanie ryzyka** – proces identyfikowania i analizy ryzyka oraz jego oceny.

25. **Użytkownik** - osoba posiadająca dostęp do danych osobowych przetwarzanych w Jednostce.
26. **Użytkownik systemu informatycznego** - osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe w Jednostce.
27. **Zagrożenie** – niepożądane działanie lub sytuacja, która może niekorzystnie wpłynąć na prawidłowość oraz bezpieczeństwo procesów realizowanych w Jednostce, potencjalna przyczyna wystąpienia incydentu.
28. **Zarządzanie ryzykiem** – skoordynowane działania w celu systematycznego stosowania zasad zarządzania, procedur, instrukcji a także kierowanie i sterowanie Jednostką z uwzględnieniem oszacowanego ryzyka.
29. **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.

Rozdział II
Ochrona Danych Osobowych
Art. 5. Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych

1. Administrator

1) wdraża odpowiednie środki techniczne i organizacyjne, mające na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych;
2) wyznacza IOD, o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych;
3) podejmuje odpowiednie działania w przypadku naruszenia ochrony danych osobowych lub podejrzenia naruszenia ochrony danych osobowych zgodnie z procedurą stanowiącą integralną część Polityki ochrony danych osobowych;
4) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie;
5) nadaje lub zatwierdza Użytkownikom uprawnienia do pracy w systemach informatycznych wykorzystywanych przez Jednostkę;
6) podejmuje decyzje dotyczące przeprowadzenia oceny skutków planowanych

operacji przetwarzania danych po konsultacji z IOD;

7) zatwierdza Rejestr czynności przetwarzania danych osobowych oraz Rejestr wszystkich kategorii czynności przetwarzania;
8) wdraża Politykę ochrony danych wraz z załącznikami;
9) dopełnia wszelkich pozostałych obowiązków wymaganych przez RODO i inne przepisy regulujące zasady przetwarzania danych osobowych w Jednostce;
10) publikuje dane kontaktowe IOD i zawiadamia o nich organ nadzorczy, zgodnie z art. 37 ust. 7 RODO. Publikacja danych kontaktowych odbywa się w poprzez publiczne udostępnienie przez Administratora informacji o: imieniu i nazwisku Inspektora, numerze kontaktowym lub adresie e-mail, zgodnie z art. 11 w zw. z art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
11) włącza i współpracuje z IOD we wszystkich sprawach dotyczących ochrony danych osobowych, w tym informuje go o nowych procesach przetwarzania danych osobowych;
12) w momencie projektowania / planowania nowych działań, które będą wiązały się z bezpośrednio lub pośrednio z przetwarzaniem danych osobowych (tzw. privacy by design) zobligowany jest do:
    a) przedstawienia opisu planowanego procesu przetwarzania danych osobowych i dokonania przy ewentualnej współpracy z IOD analizy zawierającej:
        - szczegółową podstawę prawną podjęcia działań w projektowanym procesie, w tym w odniesieniu do podstawy legalizującej przetwarzanie danych osobowych (art. 6 ust. 1 lub 9 ust. 2 RODO),
        - zakres kategorii osób oraz rodzaju danych osobowych, które będą przetwarzane w planowanym procesie,
        - przewidywane zasoby techniczno-organizacyjne (tj. materialne, sprzętowe oraz osobowe),
        - proponowane zabezpieczenia techniczno-organizacyjne,
        - planowane terminy retencji danych,
        - potencjalne ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze w odniesieniu do zagrożeń wewnętrznych i zewnętrznych,

- potencjalnych odbiorców gromadzonych danych osobowych;

b) przedstawienia IOD informacji, o których mowa w pkt a) w celu przeprowadzenia analizy ryzyka.

2. Inspektor Ochrony Danych /IOD/

1) weryfikuje przestrzeganie przepisów o ochronie danych osobowych i informuje Administratora oraz wszystkie osoby przetwarzające dane o spoczywających na nich obowiązkach;
2) wspólnie z Administratorem aktualizuje dokumentację z zakresu ochrony danych osobowych, tj. m.in. Politykę ochrony danych osobowych;
3) opracowuje Rejestr czynności przetwarzania danych oraz Rejestr wszystkich kategorii czynności przetwarzania we współpracy z Administratorem lub wyznaczonymi osobami działającymi z upoważnienia Administratora, a także dokonuje ich aktualizacji;
4) współpracuje z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych oraz monitoruje jej wykonanie;
5) pełni funkcję punktu kontaktowego oraz współpracuje w przypadkach opisanych w przepisach z Prezesem Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych;
6) dokonuje analizy zgłoszonych naruszeń ochrony danych osobowych i rekomenduje podjęcie działań w ich obsłudze;
7) na wniosek Administratora opiniuje wnioski dotyczące realizacji praw osób, których dane dotyczą;
8) we współpracy z Administratorem dokonuje systemowego sprawdzenia procesu wydawania upoważnień do przetwarzania danych osobowych i uprawnień do systemów informatycznych;
9) na wniosek Administratora opiniuje umowy powierzenia przetwarzania danych osobowych;
10) przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób mających dostęp do danych;
11) bierze czynny udział w audytach zewnętrznych dotyczących przetwarzania danych

osobowych w Jednostce.

1) **Administrator Systemów Informatycznych przydziela Użytkownikom identyfikator i hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta Użytkowników zgodnie z zasadami określonymi w Polityce ochrony danych osobowych oraz właściwych przepisach prawa;**
2) dokonuje naprawy i konserwacji sprzętu komputerowego;
3) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
4) wykonuje kopie zapasowe danych lub oprogramowania;
5) prowadzi inwentaryzację sprzętu komputerowego i oprogramowania;
6) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IOD o naruszeniu i współdziała z nim przy ustalaniu i usuwaniu skutków naruszenia;
7) prowadzi regularne przeglądy infrastruktury IT.

3. Użytkownicy

1) Użytkownicy dopuszczeni przez Administratora do przetwarzania danych osobowych, zobowiązani są do:
   a) udziału w szkoleniach z zakresu ochrony danych osobowych,
   b) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   c) niezwłocznego zawiadomienia przełożonego o naruszeniach ochrony danych osobowych,
   d) stosowania określonych przez Administratora procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym.
2) Ponadto osoby zajmujące kierownicze stanowiska w strukturze Jednostki oraz osoby zatrudnione na samodzielnych stanowiskach pracy są zobowiązane do:
   a) współdziałania z IOD w zakresie spraw dotyczących ochrony danych osobowych,

b) sprawowania nadzoru nad pracą podległych osób w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,
c) niezwłocznego zawiadomienia Administratora i IOD o naruszeniach ochrony danych osobowych.
d) informowania IOD o realizacji nowych zadań lub projektów, które wiążą się z przetwarzaniem danych osobowych.

Art. 6. Zasady ochrony danych osobowych

1. Administrator zapewnia, aby przetwarzanie danych osobowych odbywało się z poszanowaniem następujących zasad:
   1) dane osobowe muszą być przetwarzane zgodnie z prawem (legalizm);
   2) dane osobowe muszą być przetwarzane rzetelnie i uczciwie (rzetelność);
   3) dane osobowe muszą być przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą (przejrzystość);
   4) dane osobowe muszą być przetwarzane w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których dane są przetwarzane (minimalizacja);
   5) dane osobowe muszą być przetwarzane z dbałością o prawidłowość i aktualność danych (prawidłowość);
   6) dane osobowe muszą być przetwarzane nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania danych osobowych (ograniczenie przechowywania);
   7) dane osobowe muszą być przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu);
   8) dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych (bezpieczeństwo).

Art. 7. Podstawy dopuszczalności przetwarzania danych osobowych

1. Przetwarzanie danych osobowych zwykłych dopuszczalne jest tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 ust. 1 RODO.

2. W przypadku przetwarzania szczególnych kategorii danych osobowych podstawą dopuszczalności przetwarzania danych mogą być wyłącznie przesłanki wynikające z art. 9 ust. 2 RODO.
3. W przypadku przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych powinna zostać spełniona jedna z przesłanek wymienionych w art. 10 RODO.
4. W przypadku przetwarzania danych osobowych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, którego wzór stanowi **załącznik nr 1** do Polityki (wzór służy do konstruowania szczegółowych zgód na przetwarzanie danych osobowych), wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych znajduje się w **załączniku nr 2**.

Art. 8. Obowiązek informacyjny przy przetwarzaniu danych

1. Administrator realizuje obowiązek informacyjny w stosunku do osób fizycznych od których bezpośrednio są zbierane dane osobowe zgodnie z art. 13 ust. 1 i 2 RODO oraz w stosunku do osób, których dane zostały zebrane z innego źródła aniżeli bezpośrednio od osoby, której dane dotyczą zgodnie z art. 14 ust.1 i 2 RODO.
2. Zwolnienie z realizacji obowiązku informacyjnego wynikającego z art. 13 ust. 1 i 2 RODO znajduje zastosowanie w sytuacji, gdy osoba, której dane dotyczą dysponuje już tymi informacjami oraz w przypadkach uregulowanych w powszechnie obowiązujących przepisach prawa.
3. Wzór ogólny klauzuli informacyjnej zawierającej informacje, o których mowa w art. 13 ust. 1 i 2 RODO - służącej za podstawę do konstruowania szczegółowych klauzul informacyjnych na potrzeby Jednostki, stanowi **załącznik nr 3** do niniejszej Polityki.
4. Administrator realizuje obowiązek informacyjny z art. 13 ust. 1 i 2 RODO w następujący sposób:
   1) Poprzez umieszczenie informacji w BIP

oraz w sposób szczegółowo wskazany w źródłach prawa powszechnie obowiązującego.

5. Wzór ogólny klauzuli informacyjnej - zawierającej informacje, o których mowa w art. 14 ust. 1 i 2 RODO służącej za podstawę do konstruowania szczegółowych klauzul informacyjnych na potrzeby Jednostki, stanowi **załącznik nr 4** do Polityki.
6. Zwolnienie z realizacji obowiązku informacyjnego na podstawie art. 14 ust.1 i 2, RODO znajduje zastosowanie w sytuacji, gdy zostanie spełniona jedna z przesłanek wyszczególnionych w art. 14 ust. 5 RODO.
7. Administrator realizuje obowiązek informacyjny z art. 14 ust. 1 i 2 RODO w następujący sposób:

   1.Poprzez umieszczenie informacji w BIP

   oraz w sposób szczegółowo wskazany w źródłach prawa powszechnie obowiązującego.

Art. 9. Prawa osób, których dane dotyczą

1. Osobie, której dane są przetwarzane, przysługują następujące prawa:
   1) prawo dostępu do danych;
   2) prawo do sprostowania danych;
   3) prawo do usunięcia danych;
   4) prawo do ograniczenia przetwarzania danych;
   5) prawo do przenoszenia danych;
   6) prawo do sprzeciwu;
   7) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
2. Szczegółowe zasady realizowania ww. praw zostały opisane w **załączniku nr 5**

do Polityki.

Art. 10. Procedura nadawania upoważnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą mieć dostęp osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych nadane przez Administratora, przy czym osoby te zobowiązane są złożyć oświadczenie o zachowaniu w tajemnicy danych osobowych lub winny podlegać odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
2. Administrator przygotowuje stosowne upoważnienie do przetwarzania danych osobowych na podstawie wniosku skierowanego przez pracownika ds. kadr i zatrudnienia Wzór wniosku o nadanie/zmianę/odebranie upoważnienia stanowi **załącznik nr 6** do Polityki.
3. Upoważnienie jest przygotowywane na podstawie wzoru upoważnienia do przetwarzania danych osobowych stanowiącego **załącznik nr 7** do Polityki. Administrator przed dopuszczeniem Użytkownika do przetwarzania danych osobowych zobowiązany jest do odebrania od niego oświadczenia o zachowaniu w tajemnicy danych osobowych, którego wzór stanowi **załącznik nr 8** do Polityki.
4. Administrator uprawniony jest do odwołania nadanego upoważnienia do przetwarzania danych osobowych w każdym czasie.
5. Zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych pracownik ds. kadr i zatrudnienia rejestruje w ewidencji osób upoważnionych do przetwarzania danych, której wzór stanowi **załącznik nr 9** do Polityki.
6. Upoważnienia do przetwarzania danych osobowych przechowywane są w aktach osobowych pracownika.
7. W przypadku zmiany stanowiska lub zakresu obowiązków osoby upoważnionej albo w przypadku wystąpienia innych okoliczności, które wpływają bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, pracownik ds. kadr i zatrudnienia wnioskuje do Administratora o zmianę upoważnienia i przekazuje wniosek do Administratora. Osoba, o której mowa w ust. 2 zobowiązana jest do przygotowania nowego upoważnienia do przetwarzania danych osobowych.

8. Informacja o zmianie stanowiska lub zakresu obowiązków osoby upoważnionej bądź wystąpienia innych okoliczności mających wpływ na rodzaj i zakres przetwarzanych danych osobowych, powinna być niezwłocznie przekazana do Obsługi informatycznej Jednostki celem ewentualnej zmiany uprawnień do pracy w systemach informatycznych.
9. W przypadku ustania zatrudnienia lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia, pracownik ds. kadr i zatrudnienia odnotowuje zmiany w ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 9** do Polityki. Powyższe dotyczy każdej formy zatrudnienia, a także przetwarzania danych osobowych w związku z organizacją w Jednostce stażu, praktyki, wolontariatu.
10. Informacja o ustaniu zatrudnienia osoby upoważnionej lub zaistnieniu innej przyczyny skutkującej odwołaniem upoważnienia powinna zostać niezwłocznie przekazana do Obsługi informatycznej Jednostki celem odebrania takiej osobie wszystkich uprawnień do pracy w systemach informatycznych.

Art. 11. Rejestrowanie czynności przetwarzania danych

1. Wszystkie czynności przetwarzania realizowane przez Administratora zamieszcza się w Rejestrze czynności przetwarzania danych osobowych, który w celu jego obowiązywania wprowadza się odrębnym aktem administracyjnym.
2. Wszystkie czynności przetwarzania powierzone Administratorowi przez innego Administratora, Jednostka zamieszcza w Rejestrze wszystkich kategorii czynności przetwarzania, który w celu jego obowiązywania wprowadza się odrębnym aktem administracyjnym.
3. W przypadku zmian w przepisach prawa lub nałożenia na Jednostkę przez naczelne lub centralne organy administracji państwowej obowiązku wykonania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej, w związku z realizacją których występuje konieczność przetwarzania danych osobowych, pracownicy uzyskujący taką informację zobowiązani są do poinformowania przełożonego / kierownika komórki organizacyjnej Jednostki, który we współpracy z IOD, na podstawie przekazanych informacji dokonuje uzupełnienia lub zmian w Rejestrze czynności przetwarzania danych osobowych.

4. W przypadku uzyskania informacji przez pracownika Jednostki o powierzeniu przetwarzania danych osobowych Jednostce – na podstawie umowy lub innego instrumentu prawnego – pracownik ten jest zobowiązany do poinformowania przełożonego / kierownika komórki organizacyjnej Jednostki, który we współpracy z IOD, na podstawie przekazanych informacji dokonuje uzupełnienia lub zmian w Rejestrze wszystkich kategorii czynności przetwarzania
5. Rejestry, o których mowa w ust. 1 i 2 przyjmują formę pisemną, jak również formę elektroniczną, która powinna być prowadzona w systemie informatycznym równolegle z formę pisemną.
6. Administrator jest zobowiązany do udostępnienia ww. rejestrów na żądanie organu nadzorczego. Ww. rejestry nie stanowią dokumentów udostępnianych na podstawie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2022 r., poz. 902).
7. IOD we współpracy z Administratorem, przygotowuje i aktualizuje rejestry, o których mowa w ust. 1 i 2.

Objaśnienie:

Rejestr czynności przetwarzania danych osobowych prowadzony jest przez Jednostkę w przypadku, w którym Jednostka występuje jako Administrator danych osobowych.

W Rejestrze tym zamieszcza się następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela Administratora oraz Inspektora ochrony danych,
b) cele przetwarzania,
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
e) 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,

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Rejestr wszystkich kategorii czynności przetwarzania prowadzony jest przez Jednostkę, w przypadku, w którym Jednostka występuje jako Podmiot przetwarzający dane osobowe na zlecenie.

W Rejestrze tym zamieszcza się wszystkie następujące informacje:

a) 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,
b) kategorie przetwarzań dokonywanych w imieniu każdego z Administratorów,
c) 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,
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Art. 12. Szkolenia z zakresu ochrony danych osobowych

1. Każda osoba, która uzyskuje upoważnienie do przetwarzania danych osobowych ma obowiązek zapoznać się z najważniejszymi informacjami o obowiązkach związanych z przetwarzaniem danych osobowych. Wzór informatora zawierającego ww. informacje stanowi **załącznik nr 10** do Polityki.
2. IOD lub inna wyznaczona osoba, z własnej inicjatywy lub na wniosek Administratora, przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób je przetwarzających.
3. Dodatkowo szkolenia wewnętrzne są przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych, odpowiednio uwzględniając postanowienie ust. 2.

4. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentów potwierdzających uczestnictwo w takim szkoleniu przez jego uczestników (lista obecności lub zaświadczenie/certyfikat imienny dla Użytkownika).

Art. 13. Dostęp do danych osobowych przez podmioty trzecie

1. Administrator może przekazać podmiotowi trzeciemu (niebędącemu osobą, której dane dotyczą) przetwarzane przez siebie dane osobowe w ramach:
   1) udostępnienia - jeżeli jest to przewidziane w powszechnie obowiązujących przepisach prawa;
   2) powierzenia - jeżeli podmiot trzeci przetwarza dane w imieniu Administratora i na jego udokumentowane polecenie w rozumieniu art. 28 RODO.
2. W przypadku powierzenia przetwarzania danych konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem a Podmiotem przetwarzającym dane na zlecenie, który przetwarza dane w imieniu Administratora (zwanym również Procesorem) bądź posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno Podmiot przetwarzający jak i Administratora.
3. Administrator przed powierzeniem przetwarzania danych osobowych zobligowany jest do uzyskania informacji o stosowanych przez Procesora środkach technicznych i organizacyjnych, za pomocą listy kontrolnej procesora stanowiącej **załącznik nr 11** do Polityki.
4. IOD przygotowuje (we współpracy z osobami upoważnionymi, a także osobą reprezentującą Administratora) i weryfikuje umowy powierzenia przetwarzania danych lub inne instrumenty prawne przed ich zawarciem.
5. Administrator przyjął minimalne wymagania co do treści umowy powierzenia przetwarzania danych, której wzór stanowi **załącznik nr 12** do Polityki.
6. Administrator po zawarciu każdej umowy powierzenia – za pośrednictwem pracownika ds. kadr i zatrudnienia – odnotowuje ten fakt w rejestrze zawartych umów powierzenia, którego wzór stanowi **załącznik nr 13** do Polityki.

Art. 14. Sposób weryfikacji Podmiotu Przetwarzającego (Procesora)

1. W przypadku powierzenia przetwarzania danych konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem a Podmiotem przetwarzającym dane na zlecenie, który przetwarza dane w imieniu Administratora (zwanym również Procesorem) bądź posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno Podmiot przetwarzający jak i Administratora.
2. Administrator przed powierzeniem przetwarzania danych osobowych zobligowany jest do uzyskania informacji o stosowanych przez podmiot, któremu zamierza powierzyć dane osobowe środkach technicznych i organizacyjnych, za pomocą listy kontrolnej stanowiącej **załącznik nr 11** do Polityki. Lista kontrolna powinna zostać przekazana potencjalnemu Podmiotowi przetwarzającemu na etapie negocjowania umowy na świadczenie usług.
3. W przypadku wątpliwości w zakresie udzielonych przez potencjalny Podmiot przetwarzający informacji w liście kontrolnej, Jednostka powinna dokonać konsultacji z IOD czy ww. podmiot zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymogi rozporządzenia RODO i chroniło prawa osób, których dane dotyczą.
4. IOD przygotowuje (we współpracy z osobami upoważnionymi, a także osobą reprezentującą Administratora) i weryfikuje umowy powierzenia przetwarzania danych lub inne instrumenty prawne przed ich zawarciem.
5. Administrator przyjął minimalne wymagania co do treści umowy powierzenia przetwarzania danych, której wzór stanowi **załącznik nr 12** do Polityki.
6. W przypadku kiedy odpowiedzi udzielone przez Podmiot przetwarzający wskazują iż nie ma od wdrożonych żadnych środków technicznych, administrator decydując się na powierzenie przetwarzania danych określa minimalne zabezpieczenia które musi wdrożyć podmiot przetwarzający, w umowie powierzenia przetwarzania danych osobowych.

Art. 15. Jednostka w roli Podmiotu przetwarzającego (Procesora)

1. Jednostka, w związku z powierzeniem przetwarzania danych osobowych przez inny podmiot (odrębnego Administratora) występuje w roli Podmiotu przetwarzającego (Procesora), o którym mowa w art. 4 pkt 8 RODO.
2. Powierzenie zadań przez inny podmiot powinno nastąpić na mocy zawartej umowy powierzenia danych, o której mowa w art. 28 ust. 3 RODO lub innego instrumentu prawego.
3. Jednostka występująca w roli Podmiotu przetwarzającego (Procesora) zobowiązana jest stosować środki techniczne i organizacyjne aby zapewnić powierzonym danym należytą ochronę zgodnie z art. 24 i 32 RODO.
4. Szczegółowe obowiązki dotyczące ochrony danych osobowych powinna regulować umowa powierzenia przetwarzania danych, o której mowa w pkt 2 niniejszego artykułu.

Art. 16. Zasady anonimizacji danych osobowych

1. Osoba sporządzająca dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki jest zobowiązana do ich oceny pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.
2. Osoba sporządzająca dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki jest zobowiązana do dokonania analizy legalności publikacji danych osobowych zawartych w dokumentach oraz w razie konieczności do dokonania ich anonimizacji.
3. Na podstawie obowiązujących przepisów o dostępie do informacji publicznej zaleca się stosowanie następujących zasad anonimizacji danych, z uwzględnieniem wyjątków wynikających z przepisów prawa:
   1) w przypadku udostępniania informacji o osobie fizycznej anonimizacji – co do zasady – podlegają:
      a) imię i nazwisko, chyba że dane te są zawarte w umowach podlegających publikacji w Biuletynie Informacji Publicznej,
      b) numer PESEL oraz NIP,
      c) data i miejsce urodzenia,

d) numer dokumentu, za pomocą którego można zidentyfikować osobę fizyczną (np. dowód, paszport, prawo jazdy, legitymacja, koncesja itp.),
e) adres zamieszkania, zameldowania lub pobytu,
f) numer telefonu lub faksu,
g) adres e-mail,
h) numer rachunku bankowego,
i) numer działki i obręb,
j) numer księgi wieczystej,
k) informacje o zobowiązaniach finansowych (chyba że dane te podlegają publikacji w Biuletynie Informacji Publicznej),
l) informacje o stanie zdrowia, sytuacji finansowej, społecznej itp.,
m) inne dane pozwalające zidentyfikować osobę fizyczną lub naruszyć jej prawa i wolności;

2) w przypadku udostępniania wyciągów z rachunków bankowych lub dokumentacji księgowej (w tym faktur) anonimizacji podlegają:
a) imię i nazwisko (chyba że dane te są zawarte w umowach podlegających publikacji w Biuletynie Informacji Publicznej),
b) numer PESEL oraz NIP,
c) adres zamieszkania, zameldowania lub pobytu,
d) numer rachunku bankowego;

3) anonimizacji nie podlega natomiast imię i nazwisko usługodawcy lub nazwa firmy realizującej usługę, informacja o wykonanej usłudze oraz kwota, za jaką usługa została wykonana;

4) w przypadku udostępniania kopii innych dokumentów Jednostki dodatkowo anonimizacji podlegają wszystkie informacje, które mogą bezpośrednio zidentyfikować osobę fizyczną lub inne osoby fizyczne biorące udział w realizacji spraw.

4. Opisane wyżej zasady anonimizacji należy traktować jako reguły ogólne anonimizacji, które powinny być każdorazowo indywidualnie weryfikowane w przypadku udostępniania danych.
5. Anonimizacji nie podlegają w żadnym przypadku:
1) nazwy organów, urzędów oraz instytucji publicznych;

2) nazwy organizacji międzynarodowych;
3) nazwy sądów;
4) nazwy spółek Skarbu Państwa;
5) dane osób reprezentujących Administratora;
6) dane pracowników Administratora w zakresie realizacji zadań określonych w regulaminie Jednostki;
7) dane członków zespołów, komisji, rad i innych powołanych do realizacji zadań;
8) nazwy dokumentów np. uchwała, zarządzenie, umowa, porozumienie, aneks, a także elementy dokumentów, które nie naruszają praw i wolności osoby;
9) imiona i nazwiska autorów cytowanych książek, komentarzy, artykułów naukowych, jeśli ich prace były wykorzystywane w treści dokumentów urzędowych podlegających udostępnieniu;
10) oznaczenie czasu tj. informacje o latach, miesiącach, dniach, godzinach, przedziałach czasowych, jak też daty wytworzenia dokumentów, z wyjątkiem daty urodzenia osoby fizycznej;
11) dane, co do których wyrażona jest pisemna zgoda na ich ujawnienie w Biuletynie Informacji Publicznej (np. petycje).

Art. 17. Procedura przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej

1. Administrator udostępnia publicznie dane osobowe w Biuletynie Informacji Publicznej zgodnie z zasadami określonymi w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2022 r. poz. 902) i innych przepisach prawa powszechnie obowiązującego.
2. Administrator, z uwzględnieniem zasady ograniczenia przechowywania zapewnia, że przechowuje dane osobowe publikowane w Biuletynie Informacji Publicznej w formie umożliwiającej identyfikację podmiotu danych przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane (okres retencji).
3. W przypadkach, gdy okres retencji danych osobowych publikowanych w Biuletynie Informacji Publicznej nie wynika wyraźnie z przepisów prawa, Administrator ustala

niniejsze okresy samodzielnie, uwzględniając ogólne zasady przetwarzania danych osobowych przewidziane w RODO, w tym przede wszystkim zasadę ograniczenia przechowywania określoną w art. 5 ust. 1 lit. e. Wszystkie ustalone okresy retencji zostają uwzględnione w treści Rejestru czynności przetwarzania danych osobowych prowadzonego przez Administratora, zwanego dalej Rejestrem.

4. Dane osobowe mogą być przetwarzane dłużej niż wynosi okres retencji w przypadku, gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (na zasadach określonych w art. 89 ust. 1 RODO) pod warunkiem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności podmiotów danych.
5. Administrator – za pośrednictwem pracownika księgowości cyklicznie tj. nie rzadziej niż od 1 do 14 lipca każdego roku posiada obowiązek dokonania przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej. Poza okresowymi przeglądami Administrator przeprowadza również przeglądy ww. danych, jeśli zajdzie przynajmniej jedna z poniższych sytuacji:
   1) zmienione zostaną powszechnie obowiązujące przepisy prawa mające wpływ na okres retencji;
   2) organ nadzorczy lub organ kontrolujący wydadzą zalecenia dotyczące przeglądu danych;
   3) zostanie wydana uzasadniona decyzja Administratora, o której zostaną poinformowane osoby zatrudnione w organizacji Administratora oraz z nią współpracujące.

6. Wszelkie przeglądy danych osobowych publikowanych w Biuletynie Informacji Publicznej podlegają udokumentowaniu w postaci stosownego dokumentu i są przechowywane w dziale księgowości. Art. 18. Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu informatycznego Jednostki oraz wszelkich innych dokumentów zawierających dane osobowe, osoby upoważnione są zobowiązane do zachowania następujących środków

ostrożności:

1) wydruki z systemu informatycznego i wszelkie inne dokumenty zawierające dane osobowe powinny być niedostępne dla osób nieuprawnionych;
2) wydruki z systemu informatycznego i wszelkie inne dokumenty zawierające dane osobowe nie mogą być pozostawione w drukarce lub kserokopiarce ogólnodostępnej;
3) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki właściwej klasy;
4) dokumenty zawierające dane osobowe, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

Art. 19. Naruszenia ochrony danych osobowych

1. Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych.
2. Procedura zarządzania naruszeniami ochrony danych stanowi **załącznik nr 14** do Polityki.

Rozdział III
Procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Art. 20. Zasady zarządzania uprawnieniami Użytkowników w systemach informatycznych

1. Obsługa informatyczna Jednostki na wniosek lub ustną dyspozycję pracownika ds. kadr iatrudnienia utworzy konta dostępu do systemów informatycznych i poszczególnych modułów. Uzupełniony wniosek następnie zatwierdzany jest przez Administratora, który nadaje uprawnienia Użytkownikom do pracy w systemach informatycznych i poszczególnych modułach – wzór wniosku o nadanie/zmianę/odebranie uprawnień

stanowi **załącznik nr 15** do Polityki.

2. Obsługa informatyczna Jednostki dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień Użytkowników systemów informatycznych na podstawie wniosku, złożonego przez osobę, o której mowa w ust. 1 i zatwierdzonego przez Administratora.
3. Pracownik ds. kadr i zatrudnienia wpisuje do ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 9** oraz do upoważnienia do przetwarzania danych - **załącznik nr 7** systemy informatyczne do jakich osoba upoważniona do przetwarzania danych otrzymała dostęp. W przypadku zmiany lub odebrania uprawnień ww. informacja jest odnotowywana w ewidencji osób upoważnionych do przetwarzania danych osobowych w kolumnie „Dostęp do systemów informatycznych z uprawnieniami".

Art. 21. Zasady zabezpieczenia dostępu do systemów informatycznych

1. W przypadku dostępu Użytkowników do systemów informatycznych (dziedzinowych i operacyjnych) należy stosować metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/login-u oraz hasła.
2. Hasło powinno składać się z unikalnego zestawu znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne. Hasło powinno być regularnie zmieniane przez Użytkownika oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej. Hasło co do zasady powinno się składać z minimum 12 znaków i być zmieniane co min. 180 dni. Hasła do systemów dziedzinowych powinny być tworzone w schemacie określonym przez dostawcę oprogramowania.
3. Użytkownik zobowiązany jest do zachowania poufności hasła i niezapisywania go w sposób jawny.
4. Hasła administracyjne do urządzeń i systemów informatycznych, w tym baz danych, winny być przechowywane w zapieczętowanej kopercie w miejscu wskazanym przez Administratora lub w formie elektronicznej na szyfrowanym nośniku danych.

Art. 22. Zasady zarządzania sprzętem elektronicznym i oprogramowaniem

1. Użytkownik zobowiązany jest korzystać ze sprzętu elektronicznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
2. Użytkownik ma obowiązek niezwłocznie zgłosić Administratorowi utratę lub zniszczenie powierzonego sprzętu.
3. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać do systemu informatycznego niezatwierdzonych urządzeń.
4. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive'y) do wykonywania zadań służbowych. Szczegółowa procedura użytkowania prywatnych urządzeń elektronicznych przy pracy zdalnej stanowi **załącznik nr 16** do Polityki.
5. Administrator ma prawo do monitorowania sprzętu służbowego wykorzystywanego przez Użytkowników. O fakcie monitorowania Administrator zobowiązany jest powiadomić Użytkowników, zgodnie z przepisami Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2023 r. poz. 1465) nie później niż 2 tygodnie przed jego uruchomieniem.
6. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Jednostce.

Art. 23. Zasady wykonywania kopii bezpieczeństwa

1. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania Jednostki tworzy się kopie zapasowe danych.
2. Kopią zapasową objęte są: ……..
3. Kopią zapasową objęte są: systemy informatyczne mające wpływ w szczególności na zachowanie ciągłości działania, oraz inne zasoby, w których gromadzone są dane istotne dla Administratora.

Zakres kopii	Częstotliwość wykonywania	Forma wykonania (automat/ ręcznie)	Urządzenia na które wykonywana jest kopia
Bazy danych systemów dziedzinowych (Budżet, Środki trwałe, Płatnik)	Dni robocze	Automat	pendrive

4. Kopie zapasowe nie powinny znajdować się w tym samym pomieszczeniu co dane źródłowe.
5. Za sporządzenie kopii zapasowych odpowiedzialna jest Obsługa informatyczna Jednostki.
6. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych dokumentów znajdujących się na lokalnych dyskach twardych.
7. Obsługa informatyczna Jednostki zobowiązana jest do testowania kopii zapasowych, w tym celu powinna:
   1) uruchomić środowisko testowe do testowania kopii zapasowej;
   2) rozpocząć proces symulacji przywracania kopii zapasowej;
   3) zweryfikować poprawność przywróconych danych;
   4) zakończyć sprawdzanie poprawności wykonanej kopii zapasowej;
   5) usunąć dane ze środowiska testowego.

Art. 24. Zasady korzystania z poczty elektronicznej

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu poczty elektronicznej wyłącznie w celu prowadzenia korespondencji służbowej.
2. Użytkownik nie może używać służbowego adresu poczty elektronicznej do celów prywatnych, w szczególności do rejestracji w serwisach społecznościowych,

dokonywania zakupów w sklepach internetowych itp.

3. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu poczty elektronicznej odbiorcy wiadomości.
4. Użytkownik podczas wysyłania wiadomości e-mail do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie wiadomości e-mail do wielu adresatów z użyciem opcji „Do wiadomości - DW".
5. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości e-mail. Zabezpieczenia kryptograficzne mogą polegać na przesłaniu zahasłowanych plików w formie załącznika, jednak hasło powinno być przekazane adresatowi za pośrednictwem innego kanału komunikacji np. wiadomości sms bądź podczas rozmowy telefonicznej przeprowadzonej po uprzednim zweryfikowaniu tożsamości adresata.
6. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, w szczególności - jeżeli nie ma pewności co do autentyczności adresata wiadomości - nie powinien otwierać plików i linków w niej zawartych, ani dołączonych załączników. Tego typu wiadomości, w większości przypadków mogą zawierać załączniki ze szkodliwym kodem, które po ich otwarciu infekują komputer Użytkownika a tym samym powodują realne ryzyko zaimplementowania kodu w pozostałych komputerach sieci wewnętrznej Jednostki.
7. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub ich zaszyfrowaniem przez kryptowirusy. W takim przypadku Użytkownik powinien niezwłocznie poinformować o zdarzeniu Administratora.
8. Użytkownik powinien regularnie przeglądać folder „Spam" i usuwać niepotrzebne wiadomości.

Art. 25. Zasady korzystania z Internetu

1. Użytkownik powinien korzystać z dostępu do sieci Internet wyłącznie w celach niezbędnych do wykonywania zadań służbowych.
2. Użytkownik nie powinien otwierać stron internetowych zawierających treści

nie związane bezpośrednio z merytoryką pracy, ze względu na możliwość przypadkowego pobrania złośliwego kodu, który może automatycznie zainfekować system operacyjny komputera.

3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane bez zgody Administratora.
4. Użytkownik nie może korzystać ze stron internetowych, na których prezentowane są treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla Użytkownika).
5. Użytkownik nie może pobierać aplikacji z sieci Internet bez wcześniejszej zgody Administratora.
6. Użytkownik, w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę internetową, powinien zwrócić uwagę na pojawienie się odpowiedniej ikony (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę „kłódki” i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Użytkownik powinien zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku) lub podania przez Internet jego loginów i haseł, PIN-ów, numerów kart płatniczych.

Art. 26. Zasady korzystania z bankowości elektronicznej

1. Użytkownik, który wykonuje przelewy bankowe zobowiązany jest do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.
2. Użytkownik zobowiązany jest do zapamiętania lub przechowywania hasła dostępu oraz innych danych służących do uwierzytelniania i autoryzacji w bezpiecznym miejscu.
3. Użytkownik nie może opuścić stanowiska pracy bez wylogowania się i zamknięcia przeglądarki internetowej.
4. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.

5. W celu zalogowania się do systemu bankowości elektronicznej Użytkownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.
6. Obsługa informatyczna Jednostki jest zobowiązana do wyposażenia komputerów służących do korzystania z bankowości elektronicznej w aktualne oprogramowanie oraz zabezpieczenia systemu na poziomie wysokim (m.in. oprogramowanie antywirusowe, włączony firewall) oraz do wykonywania okresowej kontroli zgodności ustawień sprzętu informatycznego z zasadami dotyczącymi bezpieczeństwa teleinformatycznego przekazanymi przez bank, który obsługuje bankowość elektroniczną.
7. Użytkownicy obsługujący bankowość elektroniczną są zobligowani do zapoznania się z zasadami bezpieczeństwa teleinformatycznego przekazanymi przez bank, który obsługuje bankowość elektroniczną.

Art. 27. Zarządzanie pojemnością przestrzeni dyskowej

1. W przypadku wdrażania nowej wersji oprogramowania przez Obsługę informatyczną Jednostki, konieczne jest uprzednie wykonanie niezbędnych kopii zapasowych zarówno użytkowanych systemów, jak i plików źródłowych poszczególnych Użytkowników – czyli wszystkiego co może być przydatne do zapewnienia poufności, integralności dostępności i rozliczalności.
2. Z każdej wdrożonej zmiany w wersji oprogramowania Obsługa informatyczna Jednostki jest zobowiązana sporządzić stosowną dokumentację tzw. bazę konfiguracji – raport (w wersji papierowej lub elektronicznej) pozwalającą na ewentualne przywrócenie systemów i oprogramowania do wersji sprzed zmiany, w której opisane są informacje na temat wykrytych nieprawidłowości, sugestie dot. procesu, uwagi (np. z raportów audytowych IT), które sugerują konieczność wdrożenia nowej wersji oprogramowania.
3. Co najmniej raz na pół roku Obsługa informatyczna Jednostki przeprowadza weryfikację sprzętu i oprogramowania oraz określa konieczność wprowadzenia zmian w oprogramowaniu, jeśli zaistnieje taka konieczność.

Art. 28. Zasady bezpiecznego przydzielania przestrzeni dyskowej

1. Podczas przydzielania przestrzeni dyskowej należy w sposób racjonalny przydzielać zasoby, zachowując próg ostrzegawczy na poziomie 80% zajętości przestrzeni.
2. Obsługa informatyczna Jednostki powinna wdrożyć mechanizmy umożliwiające w sposób racjonalny zarządzanie ww. przestrzenią dyskową dla każdego Użytkownika.
3. Raz na pół roku Obsługa informatyczna wykonuje analizę zajętości dysku. Do tego celu wykorzystuje wbudowane narzędzia konsoli zarządzania dyskami dostępnymi w systemach operacyjnych lub używa przeznaczonego do tego celu oprogramowania służącego do skanowania zajętości przestrzeni dyskowej.
4. W celu czyszczenia dysku ze zbędnych plików (pozostałości po działających lub odinstalowanych aplikacjach) oraz czyszczenia rejestru systemowego należy na przykład zainstalować przeznaczone do tego celu oprogramowanie, które po dokonaniu odpowiednich założeń systemowych dotyczących rozmiaru zbędnych plików umożliwi wyżej wskazane działania naprawcze.

Art. 29. Komunikacja i czynności serwisowe na odległość

1. Komunikacja z zewnątrz powinna być realizowana tylko poprzez mechanizmy szyfrujące zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer, AnyDesk). W przypadku podmiotów zewnętrznych dokonujących czynności serwisowych (np. aktualizacji oprogramowania dziedzinowego) dostęp taki jest nadzorowany przez Obsługę informatyczną Jednostki oraz każdorazowo powinien być poprzedzony autoryzacją (np. podaniem hasła do Team Viewer, które wygasa po skończonej sesji).
2. Komunikację należy prowadzić tylko za pomocą bezpiecznych metod transmisji, w tym włączenia transmisji szyfrowanej lub przeniesienia usług sieciowych na serwer posiadający taką możliwość.

Art. 30. Zasady pracy z urządzeniami mobilnymi

1. Administrator dopuszcza możliwość pracy z urządzeń mobilnych wyłącznie z urządzeń przeznaczonych do użytku służbowego.

2. Urządzenia mobilne służące do łączenia się systemami i sieciami zarządzanymi przez Administratora muszą być zgłoszone do Obsługi informatycznej Jednostki celem zabezpieczenia ich odpowiednimi środkami uwierzytelniania.
3. Administrator zabrania wykorzystywania służbowych urządzeń mobilnych do celów prywatnych oraz udostępniania ich osobom trzecim, jak również instalowania aplikacji, które nie są niezbędne do wykonywania obowiązków pracowniczych danego Użytkownika.
4. Administrator zabrania korzystania z publicznych sieci WiFi, chyba że połączenie jest dodatkowo zabezpieczone kanałem VPN oraz pozostawiania urządzenia bez nadzoru Użytkownika, w szczególności w miejscach ogólnodostępnych dla szerokiego grona osób trzecich.
5. Użytkownik nie może pozostawiać urządzenia mobilnego bez opieki, ani pożyczać go osobie trzeciej.
6. Z siecią służbową Użytkownik może łączyć się tylko za pośrednictwem urządzeń zaakceptowanych przez Administratora.
7. Użytkownik powinien używać tylko rozwiązań posiadające silne mechanizmy szyfrowania transmisji i ochrony danych.
8. Obsługa informatyczna Jednostki prowadzi ewidencję udostępnionych urządzeń mobilnych.

Art. 31. Zasady zabezpieczania sprzętu elektronicznego i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone oprogramowaniem antywirusowym, które sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu.
2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie powinno odbywać się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.
3. Obowiązkiem Obsługi informatycznej Jednostki jest nadzór nad aktualizacją oprogramowania antywirusowego.
4. Użytkownik jest obowiązany każdorazowo zawiadomić Obsługę informatyczną Jednostki o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia

wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.

5. Użytkownik, który posiada dostęp do systemów informatycznych powinien mieć zablokowaną możliwość instalowania nieautoryzowanego oprogramowania.

Art. 32. Zasady korzystania z elektronicznych nośników danych

1. Użytkownik może korzystać wyłącznie z szyfrowanych, elektronicznych nośników danych w szczególności pendrive'ów, dysków zewnętrznych, nośników optycznych przeznaczonych do użytku służbowego.
2. Użytkownik korzystający z elektronicznych nośników danych w całym okresie użytkowania odpowiedzialny jest za bezpieczeństwo danych. W przypadku zgubienia nośnika Użytkownik jest zobowiązany niezwłocznie powiadomić o tym fakcie Administratora.
3. Użytkownik korzystający z ww. urządzeń zobowiązany jest do:
   1) przechowywania danych na dysku szyfrowanym;
   2) transportu nośnika w sposób minimalizujący ryzyko kradzieży lub zniszczenia oraz stosownego jego zabezpieczenia przed uszkodzeniem;
   3) zdecydowanego i skutecznego uniemożliwienia skorzystania z nośnika osobom nieuprawnionym (np. rodzina, dzieci, znajomi).
4. Obsługa informatyczna Jednostki jest odpowiedzialna za prowadzenie inwentaryzacji sprzętu elektronicznego oraz utrzymywanie jej aktualności.

Art. 33. Zasady wykonywania przeglądów, serwisu i konserwacji sprzętu elektronicznego i nośników danych

1. Obsługa informatyczna Jednostki dokonuje przeglądu i konserwacji sprzętu elektronicznego i nośników danych.
2. Użytkownik nie może samodzielne dokonywać napraw sprzętu elektronicznego, wymiany jego podzespołów oraz wykonywać innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez

producenta sprzętu w instrukcji obsługi.

3. W przypadku serwisowania infrastruktury teleinformatycznej przez podmioty zewnętrzne, Obsługa informatyczna Jednostki wymontowuje dyski twarde przed oddaniem ich do serwisu. W sytuacji, gdy do serwisu należy oddać cały zasób z dyskiem twardym, Administrator winien trwale usunąć wszystkie dane z dysku za pomocą certyfikowanych urządzeń. Jeżeli Administrator nie ma możliwości wymontowania dysku z urządzenia lub trwałego usunięcia danych, winien on podpisać stosowną umowę powierzenia danych z firmą serwisową.
4. Użytkownik ma obowiązek niezwłocznie powiadomić Obsługę informatyczną Jednostki o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
5. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji Obsługa informatyczna Jednostki jest zobowiązana do:
   1) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych;
   2) oceny zasadności odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych, a w przypadku uzasadnionej konieczności - odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.

Art. 34. Zasada utylizacji sprzętu elektronicznego

1. W przypadku wycofania sprzętu elektronicznego z użycia, dane osobowe na nim zapisane powinny być kasowane przy użyciu przeznaczonego do tego oprogramowania do bezpiecznego usuwania danych, najlepiej za pomocą certyfikowanego urządzenia np. demagnetyzera.
2. W przypadku braku możliwości programowego usunięcia danych ze sprzętu elektronicznego podlega on fizycznemu zniszczeniu.
3. Zniszczenie sprzętu elektronicznego powinno być potwierdzane protokołem zniszczenia.

Rozdział IV

Inne środki organizacyjne i techniczne służące do zabezpieczania danych osobowych

Art. 35. Zasady bezpiecznej pracy

1. Każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych, zobowiązana jest do stosowania następujących zasad bezpieczeństwa:
   1) **polityki „czystego biurka”** - w trakcie pracy na biurku powinny znajdować się tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy przez osobę upoważnioną, materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każda osoba zobowiązana jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osobom nieuprawnionym;
   2) **polityki „czystego ekranu”** - w przypadku chwilowego opuszczenia stanowiska pracy każda osoba zobowiązana jest do wylogowania się z systemu, bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji osobom nieuprawnionym. Ponadto w trakcie pracy należy mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych;
   3) takiego ustawienia monitora, aby osoby niepowołane nie mogły zapoznać się z informacjami wyświetlanymi na monitorze. W przeciwnym wypadku należy wyposażyć monitor w odpowiedni filtr prywatyzujący;
   4) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w zabezpieczonych szafach, zamykanych przynajmniej na klucz;
   5) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej;
   6) zachowania w poufności wszelkich informacji, w tym danych osobowych poprzez

złożenie stosownego oświadczenia;

7) niepozostawiania klucza w drzwiach biurowych po zewnętrznej stronie pomieszczenia;
8) niepozostawiania pomieszczeń biurowych bez opieki.

Art. 36. Zarządzanie ryzykiem

1. Administrator analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zwane dalej „analizami ryzyka".
2. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.
3. Analiza ryzyka powinna zapewniać:
   1) zidentyfikowanie ryzyka;
   2) oszacowanie ryzyka z punktu widzenia następstw dla działalności Jednostki oraz prawdopodobieństwa wystąpienia takiego ryzyka;
   3) informowanie o następstwach wystąpienia ryzyka;
   4) ustanowienie priorytetów w postępowaniu z ryzykiem;
   5) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem;
   6) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.
4. Administrator dokumentuje wykonaną analizę ryzyka w postaci raportu.
5. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadkach, w których zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie oraz w każdym przypadku, gdy wymagają tego obowiązujące przepisy prawa i wytyczne Prezesa Urzędu Ochrony Danych Osobowych.

Art. 37. Audyt wewnętrzny w zakresie bezpieczeństwa informacji

1. Administrator zapewnia przeprowadzenie okresowego audytu wewnętrznego

w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok lub częściej zgodnie z powszechnie obowiązującymi w tym zakresie przepisami.

2. Z przeprowadzonego audytu powinien zostać sporządzony raport.

Art. 38. Obszar przetwarzania i zarządzanie kluczami do pomieszczeń

1. Wszystkie pomieszczenia biurowe w Jednostce co do zasady stanowią obszar przetwarzania danych osobowych.
2. Dodatkowo Administrator określił szczególne obszary przetwarzania danych objęte dodatkowymi zabezpieczeniami, do których dostęp mają tylko osoby upoważnione przez Administratora.
3. Opis środków technicznych służących do zabezpieczenia danych osobowych oraz wskazanie obszaru przetwarzania zawiera **załącznik nr 17** do Polityki.
4. Administrator wyznaczył osoby, które są upoważnione do otwierania drzwi wejściowych do budynku/budynków Jednostki oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy Jednostki. Osoby, którym Administrator powierzył klucze oraz kody cyfrowe do systemu alarmowego zobowiązane są do ich nieudostępniania osobom trzecim.
5. Klucze do poszczególnych pomieszczeń osoby upoważnione posiadają w ciągłym użyciu. Na tych osobach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, ww. osoby powinny sprawdzić stan zastosowanych zabezpieczeń.
6. Zapasowe klucze do wszystkich pomieszczeń Jednostki winny zostać odpowiednio zabezpieczone. Są one przechowywane na stanowisku pracownika ds. kadr i zatrudnienia. Każdorazowe użycie klucza zapasowego powinno być zgłoszone do osoby upoważnionej przez Administratora.
7. Zabrania się pozostawiania kluczy do pomieszczeń z obszaru przetwarzania danych w drzwiach lub w miejscach ogólnodostępnych. Pomieszczenia te powinny być zamknięte na klucz na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.
8. Zabrania się dorabiania kluczy bez zgody Administratora.

9. Zabrania się pozostawiania osób trzecich w pomieszczeniach biurowych Jednostki bez nadzoru osób upoważnionych przez Administratora.
10. Osoby upoważnione do przetwarzania danych osobowych mogą przebywać po godzinach pracy Jednostki na obszarze przetwarzania danych osobowych jedynie za zgodą Administratora.
11. W przypadkach przebywania osób upoważnionych w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora mają one obowiązek upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych mają obowiązek sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.
12. Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania określona jest w **załączniku nr 18** do Polityki.

Art. 39. Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych

1. Obowiązek uwzględnienia ochrony danych w fazie projektowania spoczywa na Administratorze. Administrator zobligowany jest do szczegółowej analizy i opisu planowanego procesu przetwarzania danych. Ponadto w przypadku, gdy do przetwarzania wykorzystywane będą narzędzia dostarczane Administratorowi przez zewnętrznych dostawców wymagane jest zaangażowanie tych podmiotów. W przypadku dostawcy będącego Podmiotem przetwarzającym uwzględnienia ochrony danych w fazie projektowania oparte jest na zasadach wynikających z art. 28 RODO.
2. Kluczowym wymogiem związanym z ochroną danych osobowych w fazie projektowania i domyślną ochroną danych jest niedopuszczenie do przetwarzania danych w sposób, który naruszałby poszczególne wymogi RODO poprzez:
    1) zebranie informacji o celach danego projektu oraz planowanych środkach realizacji tych celów;
    2) określenie adekwatnych - dla danego projektu – środków technicznych i organizacyjnych służących do ochrony danych osobowych;
    3) ocenę, czy z projektem łączą się ryzyka dla praw lub wolności i przyjęcie

określonego mechanizmu postępowania z tym ryzykiem (ocena ryzyka może doprowadzić do konieczności przeprowadzenia pełnej oceny skutków a nawet uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych);

4) przypisanie ról w organizacji w zakresie dokonywania ww. ocen;
5) przeszkolenie pracowników przed rozpoczęciem przetwarzania nowego projektu;
6) planowanie terminów retencji danych;
7) szczegółowe podstawy prawne podjęcia działań w danym procesie;
8) zidentyfikowanie potencjalnych zagrożeń wewnętrznych i zewnętrznych;
9) wskazanie potencjalnych odbiorców danych.

3. Wymóg ochrony danych osobowych w fazie projektowania wymaga nie tylko oceny danego procesu przetwarzania danych przed jego rozpoczęciem, ale także monitorowania zgodności w czasie przetwarzania. Z punktu widzenia mechanizmu oceny nowych projektów i zarządzania projektami wprowadzono Rejestr czynności przetwarzania danych, który powinien podlegać bieżącym aktualizacjom.
4. Administrator zobowiązany jest do uwzględnienia procesu w stosownych upoważnieniach dla osób obsługujących proces.
5. Administrator zobowiązany jest do przedstawienia IOD ww. informacji w celu przeprowadzenia analizy ryzyka obejmującej nowy proces.

Rozdział V

Postanowienia końcowe

Art. 40. Przetwarzanie danych osobowych w celu prowadzenia postępowań rekrutacyjnych

1. Jednostka przetwarza dane osobowe kandydatów w związku z prowadzonym postępowaniem rekrutacyjnym w zakresie niezbędnym do jego przeprowadzenia. Na podstawie art. 13 ust. 1 i 2 RODO, Jednostka realizuje w stosunku do kandydatów obowiązek informacyjny.
2. Klauzula informacyjna jest zamieszczana w treści lub jako załącznik do ogłoszenia o naborze albo pracę. Każdorazowa zmiana treści klauzuli informacyjnej zawierającej

informacje, o których mowa w art. 13 ust. 1 i 2 RODO, wymaga przeprowadzenia uprzednich konsultacji z IOD.

3. Jednostka, jako Administrator wdraża odpowiednie środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa danych osobowych kandydatów.
4. Jednostka jest zobowiązana podać do publicznej wiadomości wyniki naboru na wolne stanowisko pracy. Informacja podawana jest do publicznej wiadomości poprzez umieszczenie jej w widocznym miejscu w siedzibie Jednostki oraz w Biuletynie Informacji Publicznej.

Art. 41. Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych

1. Administrator lub osoba działająca w jego imieniu jest zobowiązany/-a poinformować IOD o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
2. W sytuacji, gdy dobór narzędzi do przetwarzania danych osobowych nastąpi w drodze wyłonienia najkorzystniejszej oferty w ramach postępowania o udzielenie zamówienia publicznego, IOD jest zawiadamiany o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przez Administratora. Zawiadomienie IOD o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej powinno zawierać m. in. informację o nazwie państwa trzeciego lub organizacji międzynarodowej, informację o celu przekazania danych osobowych, a także informację o kategorii osób, których dane dotyczą oraz ich rodzaju. Zawiadomienie przekazywane jest na adres poczty elektronicznej IOD oraz obsługi prawnej Jednostki. Informacje zawarte w zawiadomieniu są niezbędne do zweryfikowania przez IOD oraz obsługę prawną Jednostki właściwej podstawy przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
3. Na podstawie ww. informacji, IOD dokonuje aktualizacji Rejestru czynności przetwarzania danych osobowych oraz właściwych klauzul informacyjnych, o ile przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej jest dopuszczalne w świetle rozdziału V RODO. W przypadku braku podstaw do

przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, IOD oraz obsługa prawna Jednostki informuje Administratora o braku przesłanki legalizującej transfer danych osobowych.

Art. 42. E-usługi.

1. Administrator może wdrożyć i stosować narzędzia elektroniczne, środki komunikacji elektronicznej, inne środki łączności oraz usługi online w celu załatwiania spraw w kontaktach z podmiotami trzecimi m.in. na podstawie art. 14 KPA w zw. z w art. 20a ust. 1 albo 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2023 r. poz. 57 ze zm.) oraz w zw. z art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).
2. Przy wdrażaniu tego rodzaju systemów i narzędzi teleinformatycznych, Administrator ma obowiązek wydać stosowne polecenia i instrukcje w celu zapewnienia należytej ochrony danych osobowych przetwarzanych przez osoby upoważnione. Polecenia, instrukcje oraz zasady funkcjonowania systemu e-usług zostaną szczegółowo uregulowane w odrębnym dokumencie.

Art. 43. Informacje dotyczące Polityki ochrony danych osobowych

1. Każda osoba mająca dostęp do danych osobowych Jednostki jest zobowiązana zapoznać się z Polityką ochrony danych osobowych oraz potwierdzić ten fakt własnoręcznym podpisem na wykazie, którego wzór stanowi **załącznik nr 20** do Polityki.
2. Polityka winna podlegać przeglądom we współpracy z IOD i aktualizacji w przypadku zmian w otoczeniu organizacyjno-prawnym Administratora.
3. Dokument Polityki obowiązuje w wersji papierowej i znajduje się w gabinecie dyrektora
4. Przekazanie informacji o zmianach w Polityce powinno nastąpić poprzez zobowiązanie Użytkowników do zapoznania się w określonym czasie z treścią zaktualizowanej Polityki i podpisania przez nich ponownie wykazu osób zapoznanych z Polityką – **załącznik nr 20**.
5. Dokument aktualnej Polityki przechowywany jest w wersji tradycyjnej (papierowej) i

dostępny jest w Miejsko-Gminnym Zespole Oświaty. Administrator udostępnia Politykę każdemu Użytkownikowi na jego żądanie.

Art. 44. Wykaz załączników

Załącznik nr 1 – Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych.
Załącznik nr 2 – Wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych.
Załącznik nr 3 – Wzór ogólnej klauzuli informacyjnej z art. 13 ust. 1 i 2.
Załącznik nr 4 – Wzór ogólnej klauzuli informacyjnej z art. 14 ust. 1 i 2.
Załącznik nr 5 – Procedura realizacji praw osób których dane dotyczą.
Załącznik nr 6 – Wzór wniosku o nadanie/zmianę/odebranie upoważnienia do przetwarzania danych osobowych.
Załącznik nr 7 – Wzór upoważnienia do przetwarzania danych osobowych.
Załącznik nr 8 – Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych.
Załącznik nr 9 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 10 – Informator dla Użytkowników z zakresu ochrony danych osobowych.
Załącznik nr 11 – Lista kontrolna Procesora.
Załącznik nr 12 – Wzór umowy powierzenia przetwarzania danych osobowych.
Załącznik nr 13 – Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych.
Załącznik nr 14- Procedura zarządzania naruszeniami ochrony danych osobowych.
Załącznik nr 15 – Wzór wniosku o nadanie/zmianę/odebranie uprawnień w systemach informatycznych.
Załącznik nr 16 – Procedura użytkowania prywatnych urządzeń elektronicznych.
Załącznik nr 17 – Wzór opisu środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania.
Załącznik nr 18 – Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
Załącznik nr 19- Procedury ochrony danych osobowych przy pracy zdalnej.
Załącznik nr 20 – Wykaz osób zapoznanych z Polityką ochrony danych osobowych.