POLITYKA OCHRONY DANYCH OSOBOWYCH

Egzemplarz zatwierdzony: ☒ **TAK** ☐ **NIE**

Podpis Administratora:

BURMISTRZ
mgr Jerzy Bekker

.....

Spis treści

Rozdział I

Przepisy Ogólne

Art. 1. Informacje wstępne

1. Polityka ochrony danych osobowych zwana dalej „**Polityką**" jest dokumentem wewnętrznym **Urzędu Miasta i Gminy Człopa** – zwanego 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 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 2017 r., poz. 2247);
   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

Niniejsza Polityka ma zastosowanie do danych osobowych przetwarzanych w systemach informatycznych (sposób zautomatyzowany) oraz w postaci papierowej (niezautomatyzowany).

1) Środki techniczne i organizacyjne ujęte w niniejszej Polityce mają również zastosowanie do danych osobowych przetwarzanych w projektach finansowanych ze środków zewnętrznych, chyba że umowa projektowa stanowi inaczej.
2) Polityka ma także zastosowanie do danych osobowych przetwarzanych przez Jednostkę w ramach pracy zdalnej, której warunki szczegółowo określa **załącznik**

nr 17 „Procedura ochrony danych osobowych przy pracy zdalnej" do niniejszej Polityki.

3) Niniejsza Polityka ma zastosowanie do wszystkich Administratorów funkcjonujących w strukturze organizacyjnej Jednostki z uwzględnieniem przepisów krajowych.

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** – 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) **szczególnych kategorii dane osobowe**– 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 – Urząd Miasta i Gminy Człopa;**

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) **Obsługa informatyczna** – 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 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);

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 niniejszej Polityki,
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 niniejszą Politykę wraz z załącznikami,
9) dopełnia wszelkie pozostałe obowiązki wymagane przez RODO i inne przepisy regulujące zasady przetwarzania danych osobowych w Jednostce,
10) Administrator publikuje dane kontaktowe Inspektora Ochrony Danych

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 o nowych procesach przetwarzania danych osobowych,
12) Administrator 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 zawierających:
        - 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,
        - przewidywanych zasobów techniczno-organizacyjnych (tj. materialnych, sprzętowych oraz osobowych)
        - proponowanych zabezpieczeń techniczno-organizacyjnych,
        - planowanych terminów retencji danych,
        - potencjalnego 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 obowiązkach na nich spoczywających,
2) wspólnie z Administratorem aktualizuje dokumentację z zakresu ochrony danych osobowych, tj. m.in. niniejszą Polityką,

3) opracowuje Rejestr czynności przetwarzania danych oraz Rejestr wszystkich kategorii czynności przetwarzania we współpracy z Administratorem lub wyznaczonymi osobami działającymi z upoważnienia administratora i dokonuje jego 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 jego 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.

3. Obsługa informatyczna

1) 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 niniejszej Polityce oraz właściwych przepisach prawa,
2) dokonuje naprawy i konserwację 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.

4. Użytkownicy

1) Użytkownicy dopuszczeni przez Administratora do przetwarzania danych osobowych, zobowiązani są do:
   a) udziału w szkoleniach dotyczących 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 zobowiązani 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 niniejszej Polityki (wzór służy do konstruowania szczegółowych zgód na przetwarzanie danych osobowych), a 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. Administrator realizuje obowiązek informacyjny z art. 13 ust. 1 i 2 RODO w następujący sposób:
    a) co do zasady obowiązek informacyjny należy spełnić poprzez wręczanie klauzuli informacyjnej w momencie zbierania danych osobowych - w przypadku realizacji obowiązku informacyjnego na podstawie Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t. j. Dz. U. z 2020 r., poz. 256 ze zm.) organ administracji publicznej przekazuje informacje, o których mowa w art. 13 ust. 1 i 2 RODO przy pierwszej czynności skierowanej do strony, chyba że strona posiada te informacje, a ich zakres lub treść nie uległy zmianie.
    b) poprzez wywieszenie klauzuli informacyjnej, spełniającej obowiązek informacyjny, w punkcie (pokoju) przyjęć interesantów Jednostki;
    c) poprzez dołączenie klauzuli informacyjnej, spełniającej obowiązek informacyjny, do formularzy przygotowanych przez Jednostkę, dostępnych za pośrednictwem strony internetowej Jednostki lub w punktach poborów formularzy w siedzibie Jednostki;
    d) poprzez zamieszczenie klauzuli informacyjnej, spełniającej obowiązek informacyjny, w odpowiedniej zakładce Biuletynu Informacji Publicznej Jednostki lub stronie internetowej Jednostki;

    - oraz w sposób szczegółowo wskazany w źródłach prawa powszechnie obowiązującego.
4. 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 niniejszej Polityki.
5. Zwolnienie z realizacji obowiązku informacyjnego na podstawie art. 14 ust.1 i 2, RODO znajduje zastosowanie gdy zostanie spełniona jedna z przesłanek wyszczególnionych w art. 14 ust. 5 RODO.
6. Administrator realizuje obowiązek informacyjny z art. 14 ust. 1 i 2 RODO w następujący sposób:
    a) poprzez indywidualne doręczenie osobie, której dane dotyczą, klauzuli

informacyjnej, spełniającej obowiązek informacyjny, osobiście lub listownie przy pierwszej czynności skierowanej do tej osoby;

b) poprzez zamieszczenie klauzuli informacyjnej, spełniającej obowiązek informacyjny, w odpowiedniej zakładce Biuletynu Informacji Publicznej Jednostki lub stronie internetowej Jednostki;

- 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 organu nadzorczego.
2. Szczegółowe zasady realizowania w/w praw zostały opisane w **załączniku nr 5** do niniejszej 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. Pracownik Kadr przygotowuje stosowne upoważnienie do przetwarzania danych osobowych na podstawie ustnej dyspozycji Administratora.
3. Upoważnienie jest przygotowywane na podstawie wzoru upoważnienia do przetwarzania danych osobowych stanowiącego **załącznik nr 6** do niniejszej Polityki. Administrator przed dopuszczeniem Użytkownika do przetwarzania danych osobowych zobowiązany jest do odebrania oświadczenia o zachowaniu w tajemnicy danych osobowych, którego wzór stanowi **załącznik nr 7** do niniejszej 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 Kadr rejestruje w ewidencji osób upoważnionych do przetwarzania danych, której wzór stanowi **załącznik nr 8** do niniejszej Polityki.
6. Upoważnienia do przetwarzania danych osobowych przechowywane są w aktach osobowych.
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 Kadr przygotowuje nowe upoważnienie 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 celem ewentualnej zmiany uprawnień do pracy w systemach informatycznych.
9. W przypadku ustania zatrudnienia lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia, Pracownik Kadr odnotowuje zmiany w ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 8**. Powyższe dotyczy każdej formy zatrudnienia, a także przetwarzania danych osobowych w związku z organizacją stażu, praktyki, wolontariatu w Jednostce.
10. Informacja o ustaniu zatrudnienia osoby upoważnionej lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia powinna zostać niezwłocznie przekazana do Obsługi informatycznej 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 kierownika Wydziału, który we współpracy z Inspektorem Ochrony Danych, 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 kierownika Wydziału, który we współpracy z Inspektorem Ochrony Danych, 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, w tym formę elektroniczną, która powinna być prowadzona w systemie informatycznym równolegle z formę pisemną.
6. Administrator jest zobowiązany do udostępnienia w/w rejestrów na żądanie organu nadzorczego. W/w Rejestry nie stanowią dokumentów udostępnianych na podstawie Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2020 r., poz. 2176).
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 w/w informacje stanowi **załącznik nr 9** do niniejszej 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 oraz podmiotem przetwarzającym dane na zlecenie, który przetwarza dane w imieniu Administratora, 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 środkach technicznych i organizacyjnych przez procesora, za pomocą listy kontrolnej procesora stanowiącej **załącznik nr 10** do niniejszej 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 11** do Polityki.
6. Administrator po zawarciu każdej umowy powierzenia – poprzez pracownika Kadr – odnotowuje ten fakt w rejestrze zawartych umów powierzenia, którego wzór stanowi **załącznik nr 12** do niniejszej Polityki.

Art. 14. Zasady anonimizacji danych osobowych

1. Pracownicy sporządzający dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki, zobowiązani są do oceny przedmiotowych dokumentów pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.
2. Pracownicy sporządzający dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki zobowiązani są do dokonania analizy legalności publikacji danych osobowych zawartych w dokumentacji oraz w razie konieczności do dokonania ich anonimizacji.

3. Na podstawie obowiązujących przepisów o dostępie do informacji publicznej zaleca się zastosowanie następujących zasad anonimizacji danych:
   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 BIP,
      b) 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 tel. lub faksu,
      g) adres e-mail,
      h) numer konta bankowego,
      i) numer działki i obręb,
      j) numer księgi wieczystej,
      k) informacje o zobowiązaniach finansowych (chyba że dane te podlegają publikacji w BIP),
      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 BIP),
      b) PESEL oraz NIP,
      c) adres zamieszkania, zameldowania lub pobytu,
      d) numer konta bankowego,
   3) Anonimizacji nie podlega jednak 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. Zasady anonimizacji opisane w niniejszym rozdziale stanowią jedynie reguły ogólne

anonimizacji i powinny być każdorazowo indywidualnie weryfikowane kiedy dochodzi do 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 BIP (np. petycje).

Art. 15. 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 2020 r. poz. 2176) 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 ponadto 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 cyklicznie tj. nie rzadziej niż pół roku posiada obowiązek dokonania przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej. Poza okresowymi przeglądami Administrator przeprowadza również przeglądy tych 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 osoby zatrudnione w organizacji Administratora oraz z nią współpracujące zostaną poinformowane).
6. Wszelkie przeglądy danych osobowych publikowanych w Biuletynie Informacji Publicznej podlegają dokumentowaniu w postaci stosownego dokumentu.

Art. 16. Zasady dotyczące dokonywania transmisji i utrwalania obrad rady miejskiej.

1. Administrator dokonuje transmisji i utrwalania obrad rady miejskiej zgodnie z art. 20 ust. 1b ustawy o samorządzie gminnym (t. j. Dz. U. z 2020, poz. 713 ze zm.) „Obrady rady miejskiej są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk. Nagrania obrad są udostępniane w Biuletynie Informacji Publicznej i na stronie internetowej gminy oraz w inny sposób zwyczajowo przyjęty".
2. Przed rozpoczęciem obrad, Przewodniczący rady miejskiej :
   1) informuje radnych i innych uczestników, iż obrady są transmitowane na żywo oraz informuje o obowiązkach w zakresie nieujawniania, bez uzasadnionej potrzeby, danych osobowych osób niebędących funkcjonariuszami publicznymi,

niepełniącymi funkcji publicznej, ani niezwiązanymi z tą funkcją.

2) realizuje obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 RODO.

3. Administrator dokonuję teletransmisji sesji rady za pośrednictwem wyspecjalizowanej firmy Portal CRV PL indywidualnie poprzez wykupioną licencję programu komputerowego. W przypadku dokonywania transmisji i przechowywania nagrań z sesji rady miasta poprzez podmiot zewnętrzny, z którym Administrator zawarł umowę o świadczenie usługi, winna zostać zawarta również w w/w przedmiocie umowa powierzenia przetwarzania danych osobowych, a serwer podmiotu przetwarzającego winien znajdować się w na terytorium Europejskiego Obszaru Gospodarczego. W przypadku umieszczenia nagrania na serwerze państwa trzeciego należy uwzględnić wymagania stawiane w tym zakresie przez art. 44-49 RODO.
4. Administrator dysponuje własną kopią nagrania, które jest przechowywane na dwóch dyskach sieciowych.
5. Administrator dysponuje własną kopią nagrania obrad, które udostępnia na stronie internetowej Jednostki.
6. Administrator lub wyznaczona przez Administratora osoba przygotowując protokół, stenogram lub nagranie z takiego posiedzenia, w związku z jego udostępnieniem publicznym – zobowiązany jest do ochrony prawa do prywatności osób fizycznych, w tym ochrony ich danych osobowych. W związku z powyższym, jeżeli przy przygotowaniu ww. materiałów pojawią się dane osobowe osób niebędących funkcjonariuszami publicznymi, niepełniącymi funkcji publicznych, ani niezwiązanych z tymi funkcjami, powinny być one anonimizowane.
7. Administrator lub wyznaczona przez Administratora osoba dokonuje przeglądu nagrań z posiedzeń sesji rady jednostki samorządu terytorialnego, pod kątem ewentualnych nieprawidłowości związanych z brakiem anonimizacji danych osobowych osób prywatnych przed udostępnieniem nagrania z sesji na stronie internetowej i/lub w BIP-ie.
8. Powyższa zasady mają również zastosowanie do nagrań z posiedzeń innych organów władzy publicznej pochodzących z powszechnych wyborów.

Art. 17. Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu informatycznego Jednostki oraz wszelkie dokumenty zawierające dane osobowe, osoby upoważnione obowiązują następujące środki ostrożności:

1) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe powinny być niedostępne dla osób nieuprawnionych,
2) wydruki z systemu informatycznego i wszelkie 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. 18. 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 13** do niniejszej Polityki.

Rozdział III
Procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Art. 19. Zasady zarządzania uprawnieniami Użytkowników w systemach informatycznych

1. Obsługa informatyczna na podstawie ustnej dyspozycji Administratora tworzy konta dostępu do systemów informatycznych i poszczególnych modułów.
2. Obsługa informatyczna dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień Użytkowników systemów informatycznych na podstawie ustnej dyspozycji Administratora.
3. Informatyk jednostki do ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 8** – oraz do upoważnienia do przetwarzania danych - **załącznik nr 6** - wpisuje systemy informatyczne do jakich osoba upoważniona do przetwarzania danych otrzymała dostęp. W przypadku zmiany lub odebrania

uprawnień informacja ta jest odnotowywana ww. ewidencji w kolumnie „Dostęp do systemów informatycznych z uprawnieniami".

Art. 20. 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. Hasła powinny być regularnie zmieniane przez Użytkowników oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej. Hasło co do zasady powinno się składać z min. 8 znaków i powinno być zmieniane co min. 30 dni. Hasła do systemów dziedzinowych powinny być tworzone w schemacie określonym przez dostawcę oprogramowania.
3. Użytkownik zobowiązany jest do zachowania hasła w poufności i niezapisywania haseł w sposób jawny.
4. Hasła administracyjne do urządzeń i systemów informatycznych, w tym baz danych, winny być przechowywane w formie elektronicznej na szyfrowanym nośniku danych, a główne hasło zaszyfrowanej bazy przechowywane w zapieczętowanej kopercie w miejscu wskazanym przez Administratora.

Art. 21. 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 utratę lub zniszczenie powierzonego sprzętu Administratorowi.
3. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać niezatwierdzonych urządzeń do systemu informatycznego.
4. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych. Szczegółowa procedura użytkowania prywatnych urządzeń elektronicznych przy pracy zdalnej stanowi **załącznik nr 17** do

niniejszej 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 2020 r., poz. 1320 ze zm.) nie później niż 2 tygodnie przed jego uruchomieniem.
6. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Jednostce.

Art. 22. 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: systemy informatyczne mające wpływ w szczególności na zachowanie ciągłości działania, oraz inne zasoby, w których gromadzone są istotne dane dla Administratora.
3. Kopie nie powinny znajdować się w tym samym pomieszczeniu co dane źródłowe.
4. Za sporządzenie kopii zapasowych odpowiedzialna jest Obsługa informatyczna Jednostki.
5. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych dokumentów znajdujących się na lokalnych dyskach twardych w porozumieniu z obsługą informatyczną jednostki.
6. Obsługa informatyczna Jednostki zobowiązana jest do testowania kopii zapasowych, w tym celu należy:
   1) uruchomić środowisko testowe do testowania kopii zapasowej,
   2) rozpocząć proces symulacji przywracania kopii zapasowej,
   3) zweryfikować poprawność przywróconych danych,
   4) zakończyć sprawdzenie poprawności wykonanej kopii zapasowej
   5) usunąć dane ze środowiska testowego.

Art. 23. Zasady korzystania z poczty elektronicznej

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

zakupów w sklepach internetowych.

3. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy wiadomości.
4. Użytkownik podczas wysyłania maili do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
5. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości. Zabezpieczenia kryptograficzne mogą polegać na przesłaniu zahasłowanych plików w formie załącznika, niemniej hasło powinno być przekazane adresatowi za pośrednictwem innego źródła tj. sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata.
6. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, a w szczególności nie powinien otwierać plików i linków w niej zawartych, ani otwierać załączników jeżeli nie ma pewności co do autentyczności adresata wiadomości. Tego typu maile większości przypadków mogą zawierać załączniki ze szkodliwym kodem, które po „kliknięciu" infekują komputer Użytkownika oraz może istnieć 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 zaszyfrowaniem przez kryptowirusy. W takim przypadku Użytkownik powinien poinformować o zdarzeniu Administratora.
8. Użytkownik powinien regularnie przeglądać folder spam i usuwać niepotrzebne wiadomości pocztowe.

Art. 24. 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 naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.
8. Jeżeli strona internetowa podmiotu zawiera formularz kontaktowy, to taka strona powinna posiadać zabezpieczenie certyfikatem SSL, celem zaszyfrowania komunikacji pomiędzy przeglądarką internauty, a stroną internetową jednostki.

Art. 25. 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 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 przekazanymi przez bank, który obsługuje bankowość elektroniczną - zasadami dotyczącymi bezpieczeństwa teleinformatycznego.

7. Użytkownicy, obsługujący bankowość elektroniczną są zobligowani do zapoznania się z zasadami bezpieczeństwa teleinformatycznego przekazanymi przez bank, który obsługuje bankowość elektroniczną.

Art. 26. 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 wszystko 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 właściwą dokumentację, tzw. bazę konfiguracji – raport (w wersji papierowej lub elektronicznej) pozwalającej na ewentualne przywrócenie systemów i oprogramowania do wersji sprzed zmiany, w którym opisane są informacje na temat wykrytych np. nieprawidłowości, sugestii dot. procesu, uwagi (z np. raportów audytowych IT), które sugerują konieczność wdrożenia nowej wersji oprogramowania.
3. Co najmniej raz na pół roku Obsługa informatyczna wykonuje weryfikację sprzętu i oprogramowania i określa konieczność wprowadzania zmian w oprogramowaniu jeśli zaistnieje taka konieczność.

Art. 27. 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 powinna wdrożyć mechanizmy umożliwiające w sposób racjonalny zarządzanie wyżej wymienioną przestrzenią dyskową dla każdego Użytkownika.
3. Raz na pół roku Obsługa informatyczna wykonuje analizę zajętości dysku. Do tego celu Obsługa informatyczna wykorzystuje wbudowane narzędzia konsoli zarządzania dyskami dostępnymi w systemach operacyjnych lub używa dedykowanego 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 dedykowane do tego celu oprogramowanie, które po dokonaniu odpowiednich założeń systemowych dotyczących rozmiaru zbędnych plików umożliwi wyżej wymienione działania naprawcze.

Art. 28. Komunikacja i czynności serwisowe na odległość

1. Komunikacja z zewnątrz powinna być realizowana tylko poprzez mechanizmy szyfrujące zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer). W przypadku podmiotów zewnętrznych dokonujących czynności serwisowych (np. aktualizacja oprogramowania dziedzinowego) dostęp taki jest nadzorowany przez Obsługę informatyczną 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 włączenie transmisji szyfrowanej lub przeniesienie usług sieciowych na serwer posiadający taką możliwość.

Art. 29. 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, 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 danego pracownika.
4. Administrator zabrania korzystania z publicznych sieci WIFI chyba że połączenie jest dodatkowo zabezpieczone kanałem VPN, oraz pozostawiania urządzenia bez nadzoru pracownika, w szczególności w miejscach ogólnodostępnych dla szerokiego grona osób trzecich,
5. Użytkownik nie może pozostawiać urządzenia bez opieki i nie może pożyczać 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 prowadzi ewidencję udostępnionych urządzeń mobilnych.

Art. 30. Zasady zabezpieczania sprzętu elektronicznego i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone oprogramowaniem antywirusowym, który 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 jest nadzór nad aktualizacją oprogramowania antywirusowego.
4. Użytkownik jest obowiązany każdorazowo zawiadomić Obsługę informatyczną 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. 31. Zasady korzystania z elektronicznych nośników danych

1. Użytkownik może korzystać wyłącznie z szyfrowanych, elektronicznych nośników danych w szczególności pendriv-y, 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 zabezpieczenia nośnika przed uszkodzeniem,
   3) zdecydowanego i skutecznego uniemożliwienia skorzystania z nośnika osobom nieuprawnionym (np. rodzina, dzieci, znajomi).

4. Obsługa informatyczna jest odpowiedzialna za prowadzenie inwentaryzacji sprzętu elektronicznego oraz utrzymywanie jej w aktualności.

Art. 32. Zasady wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych

1. Obsługa informatyczna 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 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, Administrator winien podpisać stosowną umowę powierzenia danych z firmą serwisową.
4. Użytkownik ma obowiązek niezwłocznie powiadomić Obsługę informatyczną 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 jest zobowiązana do:
   1) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,
   2) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych, a w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.

Art. 33. Zasada utylizacji i serwisu sprzętu elektronicznego

1. W przypadku wycofania sprzętu elektronicznego z użycia, dane osobowe na nim zapisane powinny być kasowane przy użyciu dedykowanego 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. 34. 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. 35. 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. 36. 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. 37. Zarządzanie kluczami do obszaru przetwarzania danych

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 15** do niniejszej Polityki.
4. Administrator wyznaczył osoby, które są upoważnione do otwierania drzwi wejściowych do 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 nieudostępniania tych kluczy oraz kodów cyfrowych do systemu alarmowego osobom trzecim.
5. Klucze do poszczególnych pomieszczeń osoby upoważnione pobierają i zdają po zakończonym dniu pracy do sekretariatu. Od momentu pobrania kluczy do momentu ich zdania na tych osobach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, należy sprawdzić stan zastosowanych zabezpieczeń.
6. Zapasowe klucze do wszystkich pomieszczeń Jednostki winny zostać odpowiednio zabezpieczone i przechowywane są w odrębnym pomieszczeniu w metalowej gablocie. 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 ogólnie dostępnych, 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 należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy 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 16** do niniejszej Polityki.

Art. 38. 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 ochrony danych jest niedopuszczenie do przetwarzania danych w sposób, który naruszałby poszczególne wymogi RODO poprzez:
   a) zebranie informacji o celach danego projektu oraz planowanych środkach realizacji tych celów,
   b) określenie adekwatnych - dla danego projektu – środków technicznych i organizacyjnych służących do ochrony danych osobowych,
   c) ocenę czy z projektem łączą się ryzyka dla praw lub wolności i przyjęcia 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),
   d) przypisanie ról w organizacji w zakresie dokonywania w/w ocen,
   e) przeszkolenie pracowników przed rozpoczęciem przetwarzania nowego projektu.
   f) planowanych terminów retencji danych
   g) szczegółowej podstawy prawnej podjęcia działań w danym procesie
   h) potencjalnych zagrożeń wewnętrznych i zewnętrznych
   i) 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 przedstawienia Inspektorowi Ochrony Danych w/w informacji w celu przeprowadzenia analizy ryzyka obejmującej nowy proces.

Rozdział V

Postanowienia końcowe

Art. 39. 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 zamieszczona 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 urzędnicze. Informacja podawana jest do publicznej wiadomości poprzez umieszczenie jej w widocznym miejscu w siedzibie jednostki oraz w Biuletynie Informacji Publicznej.

Art. 40. Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych

1. Administrator lub osoba działająca w jego imieniu jest zobowiązana jest poinformować inspektora ochrony danych 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, inspektor ochrony danych jest zawiadamiany o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przez Informatyka Jednostki. Zawiadomienie inspektora ochrony danych o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej powinno zawierać m. in. informację o nazwie państwa trzeciego lub organizacji międzynarodowej, a także informację o celu przekazania danych osobowych; kategorii osób, których dane dotyczą oraz ich rodzaju. Zawiadomienie przekazywane jest na adres poczty elektronicznej inspektora ochrony danych oraz obsługi prawnej jednostki. Informacje zawarte w zawiadomieniu są niezbędne do zweryfikowania przez inspektora ochrony danych oraz obsługi prawnej jednostki właściwej podstawy przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
3. Na podstawie ww. informacji, inspektor ochrony danych 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, inspektor ochrony danych oraz obsługa prawna jednostki informuje administratora o braku przesłanki legalizującej transfer danych osobowych.

Art. 41. E-usługi.

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 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).

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. 42. Informacje dotyczące Polityki ochrony danych osobowych

1. Każda osoba mająca dostęp do danych osobowych Jednostki zobowiązana jest zapoznać się z niniejszą Polityką oraz potwierdzić ten fakt własnoręcznym podpisem na wykazie, którego wzór stanowi **załącznik nr 18** do niniejszej Polityki.
2. Niniejsza Polityka winna podlegać przeglądom we współpracy z Inspektorem Ochrony Danych i aktualizacji w przypadku zmian w otoczeniu organizacyjno-prawnym Administratora.
3. Dokument niniejszej Polityki obowiązuje w wersji elektronicznej oraz tradycyjnej (papierowej) i znajduje się w dyspozycji Administratora.
4. Aktualizacja Polityki odbywać się będzie centralnie, w porozumieniu z Administratorem, celem uniknięcia pomyłki, co do obowiązującej w danym momencie wersji Polityki.
5. Przekazanie informacji o zmianach powinno zostać dokonane poprzez zobowiązanie Użytkowników do zapoznania się w określonym czasie z treścią zaktualizowanej Polityki i podpisaniu przez nich ponownie wykazu osób zapoznanych z Polityką – **załącznik nr 18**.
6. Dokument aktualnej Polityki przechowywany jest w wersji tradycyjnej (papierowej) w sekretariacie Jednostki. Administrator udostępnia niniejszą Politykę każdemu Użytkownikowi na 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 upoważnienia do przetwarzania danych osobowych,

Załącznik nr 7 – Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych,
Załącznik nr 8 – Ewidencja osób upoważnionych do przetwarzania danych osobowych,
Załącznik nr 9 – Informator dla Użytkowników z zakresu ochrony danych osobowych,
Załącznik nr 10 – Lista kontrola Procesora
Załącznik nr 11 – Wzór umowy powierzenia przetwarzania danych osobowych,
Załącznik nr 12 – Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych,
Załącznik nr 13- Procedura zarządzania naruszeniami ochrony danych osobowych
Załącznik nr 14 – Procedura użytkowania prywatnych urządzeń elektronicznych,
Załącznik nr 15 – Wzór opisu środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania,
Załącznik nr 16 – Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania
Załącznik nr 17 - Procedura ochrony danych osobowych przy pracy zdalnej,
Załącznik nr 18 – Wykaz osób zapoznanych z Polityką ochrony danych osobowych.