DOM KULTURY W KRAŚNICZYNIE
ul. Polna 2a, 22-310 Kraśniczyn
NIP 5641797006, Reg. 387826792
tel. 724 191 560
e-mail: kultura@krasniczyn.art

ZARZĄDZENIE Nr 3/2021

Dyrektora Domu Kultury w Kraśniczynie

z dnia 14.04 2021 r.

w sprawie

wprowadzenia Polityki Ochrony Danych.

Na podstawie art. 24 ust. 2 Rozporządzenia 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), publ. Dz. Urz. UE L Nr 119, s. 1.

Zarządza się, co następuje:

§ 1

Wprowadza się Politykę Ochrony Danych stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
DOM KULTURY W KRAŚNICZYNIE
Marta Zorska-Swatowska
Marta Zorska-Swatowska

POLITYKA OCHRONY DANYCH OSOBOWYCH

Egzemplarz zatwierdzony: ☑ **TAK** ☐ **NIE**

Podpis Administratora:

DYREKTOR
DOM KULTURY W KRAŚNICZYNIE
Marta Zorska-Swatowska
.....

Spis treści

Rozdział I....4
Przepisy Ogólne....4
Art. 1 Informacje wstępne....4
Art. 2 Zakres stosowania Polityki....4
Art. 3 Deklaracja stosowania....4
Art. 4 Definicje....5
Rozdział II....8
Polityka Ochrony Danych Osobowych....8
Art. 5 Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych....9
1. *Administrator*....9
2. *Inspektor Ochrony Danych /IOD/*....10
3. *Użytkownicy*....11
Art. 6 Zasady ochrony danych osobowych....11
Art. 7 Podstawy przetwarzania danych osobowych....12
Art. 8 Obowiązek informacyjny przy przetwarzaniu danych....12
Art. 9 Prawa osób, których dane dotyczą....13
Art. 10 Procedura nadawania upoważnień do przetwarzania danych osobowych....14
Art. 11 Rejestrowanie czynności przetwarzania....15
Art. 12 Szkolenia z zakresu ochrony danych osobowych....17
Art. 13 Udostępnianie danych osobowych osobie, której dane dotyczą....18
Art. 14 Dostęp do danych osobowych przez podmioty trzecie....18
Art. 15 Zasady anonimizacji danych osobowych....18
Art. 16 Procedura przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej....20
Art. 17 Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe....21
Art. 18 Naruszenia ochrony danych osobowych....22
Rozdział III....22
Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych....22
Art. 19 Zasady zarządzania uprawnieniami Użytkowników w systemach informatycznych....22
Art. 20 Zasady zabezpieczenia dostępu do systemów informatycznych....23
Art. 21 Zasady zarządzania sprzętem elektronicznym i oprogramowaniem....23
Art. 22 Zasady wykonywania kopii bezpieczeństwa....24
Art. 23 Zasady korzystania z poczty elektronicznej....25
Art. 24 Zasady korzystania z Internetu....26
Art. 25 Zasady używania prywatnego sprzętu do zadań służbowych przez Użytkownika....27

Art. 26 Zasady pracy na odległość....27
Art. 27 Zasady pracy z urządzeniami mobilnymi....27
Art. 28 Zasady zabezpieczania sprzętu elektronicznego i systemu informatycznego....28
Art. 29 Zasady korzystania z elektronicznych nośników danych....29
Art. 30 Zasady wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych....29
Art. 31 Zasada utylizacji i serwisu sprzętu elektronicznego....30
Art. 32 Zasady bezpiecznej pracy....30
Art. 33 Zarządzanie ryzykiem....31
Art. 34 Audyt wewnętrzny w zakresie bezpieczeństwa informacji....32
Art. 35 Zarządzanie kluczami....32
Art. 36 Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych....33
Rozdziała IV....34
Postanowienia końcowe....34
Art. 37 Dystrybucja oraz aktualizacja Polityki....34
Art. 38 Wykaz załączników....35

Rozdział I

Przepisy Ogólne

Art. 1 Informacje wstępne

1. Polityka ochrony danych osobowych zwana dalej „Polityką" jest dokumentem wewnętrznym Domu Kultury w Kraśniczynie – 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);
   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. 2017 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 oraz w postaci papierowej będących w zasobach Jednostki.

Art. 3 Deklaracja stosowania

1. Administrator ustanawia Politykę oraz deklaruje:

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 środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym,
4) dążenie do zapewnienia poufności, dostępności oraz integralności informacji chronionych w tym szczególnie danych osobowych.

Art. 4 Definicje

1) **Administrator** – Dom Kultury w Kraśniczynie reprezentowane 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 **chyba że przepisy szczególne stanowią inaczej**; poprzez posługiwanie się w dalszej treści niniejszego dokumentu terminem „Administrator" należy rozumieć również osoby, na które Administrator delegował obowiązki przypisane mu na podstawie RODO lub innych przepisów szczególnych;
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, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4) **dane osobowe zwykłe** – wszelkie dane osobowe nienależące do szczególnych kategorii danych ani danych dotyczących wyroków skazujących lub czynów zabronionych;
5) **dane szczególnych kategorii** – 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 lub 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) **Incydent** – zdarzenia pojedyncze lub seria niepożądanych zdarzeń związanych z bezpieczeństwem danych osobowych, informacji, które zagrażają przetwarzaniu danych osobowych, informacji lub naruszają zdefiniowane wymagania bezpieczeństwa albo stwarzają znaczne prawdopodobieństwo zakłócenia w prowadzeniu działań prawnych;
8) **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";
9) **Kopia zapasowa** – kopia danych lub oprogramowania, której celem wykonania jest odtworzenie systemu po awarii;
10) **Jednostka** – Dom Kultury w Kraśniczynie, ul. Polna 2A, 22-310 Kraśniczyn**;**
11) **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;
12) **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;

13) **Obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
14) **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; ale 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;
15) **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
16) **Podatność** - właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie zaistnienia incydentu;
17) **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
18) **Polityka** – niniejsza Polityka ochrony danych osobowych, o ile co innego nie wynika wyraźnie z jej treści;
19) **Przetwarzanie** – operacje 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;
20) **Rejestr czynności przetwarzania danych** – rejestr czynności przetwarzania danych osobowych, o którym stanowi art. 30 ust. 1 RODO;
21) **Rejestr wszystkich kategorii czynności przetwarzania** – rejestr wszystkich kategorii czynności przetwarzania dokonywanych, o którym stanowi art. 30 ust. 2 RODO;
22) **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);

23) **Ryzyko** – potencjalna sytuacja, w której określone zagrożenie wykorzystując podatność aktywów lub grupy aktywów powodować może chociażby potencjalną szkodę majątkową lub niemajątkową dla Jednostki;
24) **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);
25) **Szacowanie ryzyka** – proces identyfikowania i analizy ryzyka oraz jego oceny;
26) **Użytkownik** - osoba posiadająca dostęp do dokumentacji zawierającej dane osobowe lub dostęp do systemu informatycznego przetwarzającego informacje lub 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 incydentem** - obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
29) **Zarządzanie ryzykiem** – skoordynowane działania w celu systematycznego stosowania zasad zarządzania, procedur, instrukcji a także kierowanie i sterowanie Jednostką z uwzględnieniem oszacowanego ryzyka;
30) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
31) **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

Polityka Ochrony 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 lub podejrzenia naruszenia przetwarzanych danych 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 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.

Administrator lub wyznaczona przez niego osoba:

11) 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,
12) dokonuje naprawy i konserwację sprzętu komputerowego,
13) 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,
14) wykonuje kopie zapasowe danych lub oprogramowania,
15) prowadzi inwentaryzację sprzętu komputerowego i oprogramowania,
16) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IOD o naruszeniu i współdziała z nim przy ustalaniu i usuwaniu skutków naruszenia.

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) aktualizuje dokumentację z zakresu ochrony danych osobowych, tj. m.in. niniejszą Polityką,
   3) opracowuje rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania we współpracy z Administratorem lub wyznaczonymi Użytkownikami i dokonuje jego bieżącej aktualizacji na każde żądanie Administratora,
   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) sprawuje nadzór nad zgłoszonymi do IOD naruszeniami ochrony danych osobowych,
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. 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 związanych z przetwarzaniem 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 związanych

z przetwarzaniem 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) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   2) rzetelnie i uczciwie (rzetelność);
   3) w sposób przejrzysty dla osoby, której dane dotyczą (przejrzystość);
   4) w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których dane są przetwarzane (minimalizacja);
   5) z dbałością o prawidłowość i aktualność danych (prawidłowość);
   6) nie dłużej niż potrzeba (czasowość);
   7) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

Art. 7 Podstawy 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 danych osobowych szczególnych kategorii podstawą do 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, wynikający z treści art. 13 ust. 1 i 2 RODO i służący 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:
   a) Indywidualnie w stosunku do osoby której dane dotyczą;
   b) Poprzez umieszczenie na stronie BIP Jednostki;
   c) Poprzez umieszczenie w ogólnie dostępnym miejscu w siedzibie Administratora;
   - oraz w sposoby szczegółowo wskazane w źródłach prawa powszechnie obowiązującego,
5. Wzór ogólny klauzuli informacyjnej, wynikający z treści art. 14 ust. 1 i 2 RODO i służący za podstawę do konstruowania szczegółowych klauzul informacyjnych na potrzeby Jednostki, stanowi **załącznik nr 4** do niniejszej Polityki.
6. 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.
7. Administrator realizuje obowiązek informacyjny z art. 14 ust.1 i 2 RODO w następujący sposób:
   a) Indywidualnie w stosunku do osób których dane dotyczą;
   b) Poprzez umieszczenie w ogólnie dostępnym miejscu w siedzibie Administratora;

- oraz w sposoby szczegółowo wskazane 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 wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
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 winny złożyć oświadczenie o zachowaniu w tajemnicy danych osobowych lub podlegać odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
2. Instruktor ds. kultury przygotowuje stosowne upoważnienie do przetwarzania danych osobowych.
3. Upoważnienie jest przygotowywane na podstawie wzoru upoważnienia do przetwarzania danych osobowych stanowiącego **załącznik nr 6** do niniejszej Polityki, natomiast wzór oświadczenia o zachowaniu w tajemnicy danych osobowych stanowi **załącznik nr 7**.
4. Administrator uprawniony jest do odwołania nadanego upoważnienia do przetwarzania danych osobowych w każdym czasie.
5. Zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych, Instruktor ds. kultury rejestruje w ewidencji osób upoważnionych do przetwarzania danych, której wzór stanowi **załącznik nr 8** do Polityki.

6. Upoważnienia do przetwarzania danych 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, osoba o której mowa w ust. 2 zobowiązana jest do przygotowania nowego upoważnienia do przetwarzania danych osobowych.
8. W przypadku ustania zatrudnienia lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia, Instruktor ds. kultury odnotowuje zmiany w ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 8**. Powyższe dotyczy każdej formy zatrudnienia (umowa o pracę, umowa cywilnoprawna, staż, praktyka, wolontariat i inne).
9. Informacja o ustaniu zatrudnienia osoby upoważnionej lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia powinna zostać niezwłocznie przekazana do osoby wyznaczonej przez Administratora celem odebrania takiej osobie wszystkich uprawnień do pracy w systemach informatycznych.

Art. 11 Rejestrowanie czynności przetwarzania

1. Wszystkie czynności przetwarzania realizowane przez Administratora zamieszcza się w Rejestrze czynności przetwarzania danych, który w celu jego obowiązywania wprowadza się odrębnym aktem prawa wewnętrznie obowiązującego.
2. Wszystkie czynności przetwarzania powierzone Administratorowi przez innego Administratora zamieszcza w Rejestrze wszystkich kategorii czynności przetwarzania, który w celu jego obowiązywania wprowadza się odrębnym aktem prawa wewnętrznie obowiązującego.
3. Jednostka powinna przestrzegać wszelkich zasad przetwarzania powierzonych jej danych nałożonych na podstawie obowiązujących przepisów prawa, umów powierzenia, innych instrumentów prawnych oraz dokumentach ramowych określających zasady takiego przetwarzania.
4. 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 Dyrektora, który we współpracy z Inspektorem Ochrony Danych, na podstawie przekazanych informacji dokonuje uzupełnień lub zmian w Rejestrze czynności przetwarzania danych.

5. W przypadku uzyskania informacji przez pracownika Jednostki o występowaniu tejże Jednostki jako Podmiotu przetwarzającego dane – na podstawie umowy powierzenia przetwarzania danych lub innego instrumentu prawnego – pracownik ten jest zobowiązany do poinformowania Dyrektora, który we współpracy z Inspektorem Ochrony Danych, na podstawie przekazanych informacji dokonuje uzupełnia lub zmian w Rejestrze wszystkich kategorii czynności przetwarzania
6. 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.
7. Administrator jest zobowiązany do udostępnienia w/w rejestrów na żądanie organu nadzorczego. Rejestry nie stanowią dokumentów udostępnianych na podstawie Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j . Dz. U. z 2019 r., poz. 1429) –Wyrok Wojewódzkiego Sądu Administracyjnego w Łodzi, z dnia 12 lutego 2019 r., sygn. akt II SAB/Łd 181/18.
8. IOD we współpracy z Administratorem, przygotowuje i aktualizuje rejestry, o których mowa w ust.1 i 2.

Objaśnienie:

Rejestr czynności przetwarzania danych 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.

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. Każdy Użytkownik, który 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 osoba 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 oraz zaświadczenie/certyfikat imienny dla Użytkownika)

Art. 13 Udostępnianie danych osobowych osobie, której dane dotyczą

1. Udostępnienie danych osobowych osobie, której dane dotyczą zostało opisane w **załączniku nr 5** do Polityki – art. 3 Prawo dostępu do danych.

Art. 14 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 i na udokumentowane polecenie Administratora w rozumieniu art. 28 RODO.
2. W przypadku powierzenia przetwarzania danych konieczne jest albo zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem oraz podmiotem przetwarzającym, który przetwarza dane w imieniu Administratora albo posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno podmiot przetwarzający jak i Administratora.
3. IOD przygotowuje we współpracy Użytkownikami i weryfikuje umowy powierzenia przetwarzania danych lub inne instrumenty prawne przed ich zawarciem we współpracy
   z Administratorem.
4. Administrator przyjął minimalne wymagania co do treści umowy powierzenia

przetwarzania danych, której wzór stanowi **załącznik nr 10** do Polityki.

5. Administrator po zawarciu każdej umowy powierzenia – odnotowuje ten fakt w rejestrze zawartych umów powierzenia, którego wzór stanowi **załącznik nr 11** do niniejszej Polityki.

Art. 15 Zasady anonimizacji danych osobowych

1. W przypadku dokumentów udostępnianych przez Administratora na podstawie obowiązujących przepisów o dostępie do informacji publicznej należy zastosować następujące zasady anonimizacji danych:
   1) w przypadku udostępniania informacji o osobie fizycznej anonimizacji 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.

2. Zasady anonimizacji opisane w niniejszym rozdziale stanowią jedynie reguły ogólne anonimizacji i powinny być każdorazowo indywidualnie weryfikowane kiedy dochodzi do udostępniania danych.

3. 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 (np. petycje).

Art. 16 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 2019 r. poz. 1429) i innych przepisach powszechnie obowiązującego prawa.
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. Wszystkie ustalone okresy retencji zostają uwzględnione w treści Rejestru czynności przetwarzania danych 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 – poprzez wyznaczoną osobę cyklicznie tj. raz w roku ma 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 stosownej notatki która przechowywana jest wraz z dokumentacją dotyczącą ochrony danych osobowych w gabinecie Dyrektora.

Art. 17 Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu informatycznego Jednostki, Użytkowników obowiązują następujące środki ostrożności:
   1) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe powinny być niedostępne dla osób trzecich,
   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,
   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 Prezesowi Urzędu Ochrony Danych Osobowych.
2. Procedura zgłaszania naruszeń stanowi **załącznik nr 13** do niniejszej Polityki.

Rozdział III

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Art. 19 Zasady zarządzania uprawnieniami Użytkowników w systemach informatycznych

1. Administrator lub osoba przez niego wyznaczona tworzy Użytkownikom konta dostępu do systemów informatycznych.
2. Administrator lub osoba przez niego wyznaczona dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień Użytkowników systemów informatycznych na podstawie wniosku zatwierdzonego przez Administratora.
3. W przypadku zmiany uprawnień do systemów informatycznych Administrator wydaje nowe upoważnienie do przetwarzania danych osobowych.
4. Dyrektor wpisuje systemy informatyczne do jakich osoba upoważniona do przetwarzania danych otrzymała dostęp, do ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 8** –. 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. Identyfikator jest przydzielany wg zasady przyjętej w Jednostce to jest w sposób następujący: pierwsza litera imienia i nazwisko. W identyfikatorze należy pomijać polskie znaki diakrytyczne.
3. W przypadku dublowania się identyfikatorów powinien być on rozszerzany o kolejne litery alfabetu bez polskich znaków diakrytycznych lub cyfry.
4. 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.

5. Użytkownik zobowiązany jest do zachowania hasła w poufności i niezapisywania haseł
   w sposób jawny.
6. Hasła administracyjne do urządzeń i systemów informatycznych, w tym baz danych, winny być przechowywane w zapieczętowanej kopercie w miejscu wskazanym przez Administratora.

Art. 21 Zasady zarządzania sprzętem elektronicznym i oprogramowaniem

1. Administrator prowadzi rejestr całego sprzętu informatycznego oraz wszystkich systemów i programów informatycznych w postaci książki środków trwałych.
2. Użytkownik zobowiązany jest korzystać ze sprzętu elektronicznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
3. Użytkownik ma obowiązek niezwłocznie zgłosić utratę lub zniszczenie powierzonego sprzętu Administratorowi.
4. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać niezatwierdzonych urządzeń do systemu informatycznego.
5. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych.
6. 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 2019 r., poz. 1040 ze zm) nie później niż 2 tygodnie przed jego uruchomieniem.
7. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Jednostce.
8. Użytkownik nie może instalować ani używać oprogramowania innego, niż przekazane lub udostępnione przez Administratora.

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: bazy danych programów dziedzinowych i pliki;
3. Za sporządzenie kopii zapasowych odpowiedzialna jest osoba wyznaczona przez Administratora;
4. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych dokumentów znajdujących się na lokalnych dyskach twardych;
5. Administrator lub osoba przez niego wyznaczona 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 nie może używać służbowego adresu mailowego w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
4. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy wiadomości.
5. 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".

6. 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.
7. 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.
8. 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.
9. 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 z Internetu.
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 bez zgody Administratora nie może oglądać/słuchać materiałów multimedialnych zawartych w Internecie, niezwiązanych z wykonywaniem zakresu obowiązków, co może w znacznym stopniu wysycić łącze internetowe i uniemożliwić pracę innym Użytkownikom.
6. Użytkownik nie może pobierać aplikacji z sieci Internet bez wcześniejszej zgody Administratora.
7. 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.
8. 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.

Art. 25 Zasady używania prywatnego sprzętu do zadań służbowych przez Użytkownika

1. Administrator dopuszcza możliwość korzystania z prywatnego sprzętu przez Użytkowników do wykonywania zadań służbowych, gdy zostały zastosowane następujące zabezpieczenia:
   uwierzytelnienia za pomocą loginu i hasła,
   instalacja oprogramowania antywirusowego,
   szyfrowanie danych,
   separację zasobów służbowych od prywatnych znajdujących się na sprzęcie, poprzez utworzenie zabezpieczonych odrębnych kont,
2. Administrator zobowiązuję pracowników do stosowania tożsamych zasad jak przy wykorzystywaniu sprzętu służbowego.

Art. 26 Zasady pracy na odległość

1. Komunikacja z zewnątrz powinna być realizowana tylko poprzez mechanizmy zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer). W przypadku firm 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. Administrator wprowadza obowiązek logowania połączeń wykonywanych za pomocą sieci bezprzewodowej w celu rejestracji działań Użytkowników w sieci i zmniejszenia ryzyka użytkowania sieci niezgodnie z przeznaczeniem.
3. Komunikację należy prowadzić tylko za pomocą bezpiecznych metod transmisji, w tym włączenie transmisji szyfrowanej lub przeniesienie usług sieciowych na serwer posiadający taką możliwość.

Art. 27 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, jakimi jak np. PIN-y, do zainstalowania odpowiedniego oprogramowania antywirusowego, zaszyfrowania.
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 oraz pozostawiać 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. Użytkownik powinien na bieżąco zgłaszać do Obsługi informatycznej wykonanie

aktualizacji systemu oraz aplikacji zainstalowanych na urządzeniu.

7. Z siecią firmową Użytkownik może łączyć się tylko za pośrednictwem urządzeń zaakceptowanych przez Administratora.
8. Użytkownik powinien używać tylko rozwiązania posiadające silne mechanizmy szyfrowania transmisji i ochrony danych.
9. Administrator lub osoba przez niego wyznaczona prowadzi ewidencję udostępnionych urządzeń mobilnych.

Art. 28 Zasady zabezpieczania sprzętu elektronicznego i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone programem 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 Administratora lub osoby przez niego wyznaczonej jest nadzór nad aktualizacją oprogramowania antywirusowego.
4. Użytkownik jest obowiązany każdorazowo zawiadomić Administratora lub osobę przez niego wyznaczoną 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 informatycznym powinien mieć zablokowaną możliwość instalowania nieautoryzowanego oprogramowania.

Art. 29 Zasady korzystania z elektronicznych nośników danych

1. Użytkownik może korzystać wyłącznie z elektronicznych nośników danych w szczególności pendriv-y, dysków zewnętrznych, CD-R, DVD przeznaczonych do użytku służbowego.
2. Użytkownik korzystający z elektronicznych nośników danych w całym okresie użytkowania odpowiedzialny jest za bezpieczeństwo danych.
3. Użytkownik korzystający z ww. urządzeń zobowiązany jest do:

1) przechowywania danych na dysku szyfrowanym zabezpieczonym hasłem,
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. Administrator lub osoba przez niego wyznaczona jest odpowiedzialna za prowadzenie inwentaryzacji sprzętu elektronicznego oraz utrzymywanie jej w aktualności.

Art. 30 Zasady wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych

1. Administrator lub osoba przez niego wyznaczona dokonuje przeglądu i konserwacji sprzętu elektronicznego i nośników danych.
2. Użytkownik nie może samodzielne dokonywać napraw sprzętu elektronicznego, wymiany jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
3. W przypadku serwisowania zasobów informatycznych przez podmioty zewnętrzne, Administrator lub osoba przez niego wyznaczona wymontowuje dyski twarde przed oddaniem ich do serwisu. W sytuacji, gdy do serwisu należy oddać cały zasób 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 Administrator lub osoba przez niego wyznaczona 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. 31 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.
4. W przypadku przekazywania stacji roboczej z dyskiem albo innych nośników danych do naprawy, dysk lub nośnik powinien zostać zdemontowany lub pozbawiany danych, naprawa powinna być dokonywana w obecności osoby upoważnionej przez Administratora lub powinna zostać zawarta umowa powierzenia przetwarzania danych.

Art. 32 Zasady bezpiecznej pracy

1. Każdy Użytkownik zobowiązany jest do stosowania następujących zasad bezpieczeństwa:
   1) **polityki „czystego biurka"** - w trakcie pracy Użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy Użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych,
   2) **polityki „czystego ekranu"** - w przypadku chwilowego opuszczenia stanowiska pracy Użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu

do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy Użytkownik powinien 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 po zewnętrznej stronie pomieszczenia,
8) niepozostawiania pomieszczeń biurowych bez opieki.

Art. 33 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. 34 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. Administrator dokumentuje wyniki wykonanego audytu w postaci raportu..

Art. 35 Zarządzanie kluczami

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 12** do niniejszej Polityki.
4. Administrator wyznaczył pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku Domu Kultury przed rozpoczęciem pracy jednostki. Pracownik, któremu zostały powierzone klucze zobowiązany jest do nieudostępniania kluczy osobom trzecim.
5. Klucze do poszczególnych pomieszczeń osoby upoważnione pobierają i zdają po zakończonym dniu pracy w Gabinecie Dyrektora. Od momentu pobrania kluczy do momentu ich zdania na tych osobach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń szkolnych, przed przystąpieniem do pracy, Użytkownicy sprawdzają stan zastosowanych zabezpieczeń.
6. Zapasowe klucze do wszystkich pomieszczeń Jednostki winny zostać odpowiednio zabezpieczone i przechowywane są w Gabinecie Dyrektora. Każdorazowe użycie

klucza zapasowego powinno być udokumentowane.

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 się na czas nieobecności osób upoważnionych w sposób uniemożliwiający dostęp do nich osobom trzecim.
8. Zabrania się dorabiania kluczy do pomieszczeń, kłódek, szaf biurowych itp. bez zgody Administratora.
9. Zabrania się pozostawiania osób trzecich w pomieszczeniach biurowych Jednostki bez nadzoru osób upoważnionych przez Administratora.
10. Użytkownicy po godzinach pracy Jednostki mogą przebywać na obszarze przetwarzania danych osobowych jedynie za zgodą Administratora.
11. W przypadkach przebywania Użytkowników 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.

Art. 36 Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych

1. Obowiązek uwzględnienia ochrony danych w fazie projektowania spoczywa na Administratorze. Ponadto w przypadku, gdy do przetwarzania wykorzystywane będą narzędzia dostarczane Administratorowi przez zewnętrznych dostawców wymagane jest zaangażowanie tego podmiotu. 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:
   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 przyjęcia określonego mechanizmu postepowania 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 w/w ocen,
5) przeszkolenie pracowników aby przed rozpoczęciem przetwarzania (nowego projektu).

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.

Rozdziała IV

Postanowienia końcowe

Art. 37 Dystrybucja oraz aktualizacja Polityki

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 14** do niniejszej Polityki.
2. Niniejsza Polityka winna podlegać regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym we współpracy z Inspektorem Ochrony Danych na polecenie Administratora.
3. W zależności od potrzeb mogą zostać przeprowadzone przez Inspektora Ochrony Danych także dodatkowe przeglądy Polityki z własnej jego inicjatywy, po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w strukturze Jednostki lub jego otoczeniu (nowe zagrożenia, technologie) – przy czym o wszelkich zmianach w strukturze, incydentach lub innych zagrożeniach Inspektor winien być informowany przez Administratora zgodnie z zasadami niniejszej Polityki

– lub w innych uzasadnionych przypadkach.

4. Przekazanie informacji o zmianach w Polityce 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 14**.
5. Dokument aktualnej Polityki przechowywany jest w wersji tradycyjnej (papierowej) i dostępny jest w Gabinecie Dyrektora. Administrator udostępnia niniejszą Politykę każdemu Użytkownikowi na żądanie.

Art. 38 Wykaz załączników

1) Załącznik nr 1 – Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych,
2) Załącznik nr 2 – Wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych,
3) Załącznik nr 3 – Wzór ogólnej klauzuli informacyjnej z art. 13 ust. 1 i 2,
4) Załącznik nr 4 - Wzór ogólnej klauzuli informacyjnej z art. 14 ust. 1 i 2,
5) Załącznik nr 5 – Procedura realizacji praw osób których dane dotyczą,
6) Załącznik nr 6 – Wzór upoważnienia do przetwarzania danych osobowych;
7) Załącznik nr 7 – Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych,
8) Załącznik nr 8 – Ewidencja osób upoważnionych do przetwarzania danych osobowych,
9) Załącznik nr 9 – Informator dla Użytkowników z zakresu ochrony danych osobowych,
10) Załącznik nr 10 – Wzór umowy powierzenia przetwarzania danych osobowych,
11) Załącznik nr 11 – Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych,
12) Załącznik nr 12 – Wzór opisu środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania,
13) Załącznik nr 13 – Procedura zarządzania naruszeniami ochrony danych osobowych,
14) Załącznik nr 14 – Lista osób zapoznanych z Polityką.