Regulamin Ochrony Danych Osobowych

Nazwa podmiotu wprowadzającego	Powiatowy Dom Kultury w Raciborzu
Data wprowadzenia	20 sierpnia 2025 r.
Numer zarządzenia wprowadzającego	5/2025
Podpis ADO	Robert Myśliwy
Podpis IOD	Chata Mikołajczyk Aleksandra

1. WSTĘP:

§1

Regulamin Ochrony Danych Osobowych stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad dotyczących ochrony danych osobowych dla pracowników, współpracowników oraz innych osób przetwarzających dane osobowe administratora.

§2

Regulamin Ochrony Danych Osobowych został opracowany zgodnie z wymogami 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 osobowych) (dalej „RODO"), a także ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

§3

Regulamin Ochrony Danych Osobowych stosuje się do danych osobowych przetwarzanych w systemach informatycznych, danych osobowych zapisanych na zewnętrznych nośnikach informacji, a także danych przetwarzanych w sposób tradycyjny.

§4

Każda osoba przetwarzająca dane administratora zobowiązana jest do zapoznania się z poniższym regulaminem ochrony danych osobowych oraz stosowaniem procedur i zasad w nim zawartych.

2. DEFINICJE:

Przez użyte w Regulaminie Ochrony Danych Osobowych określenia należy rozumieć:

1. **Regulamin** – Regulamin Ochrony Danych Osobowych przetwarzania danych osobowych, zwany inaczej ,,Polityką Bezpieczeństwa Ochrony Danych Osobowych",
2. **Administrator Danych Osobowych (ADO)** - podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
3. **Inspektor Ochrony Danych Osobowych (IOD)** - osoba lub podmiot wspierający administratora danych w realizacji obowiązków dotyczących ochrony danych osobowych oraz realizujący zadania, wynikające z art. 39 RODO.
4. **RODO** - 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 osobowych) (dalej ,,RODO"),
5. **Ustawa** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
6. **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, której dane dotyczą; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować,
7. **Zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
8. **Przetwarzanie danych** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany; taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnienie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowanie lub łączenie, ograniczenie, usuwanie lub niszczenie, przechowywanie, adaptowanie lub modyfikowanie
9. **Usuwanie danych** - zniszczenie danych lub ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą,
10. **Poufność danych** - zapewnienie, że dane nie są udostępniane nieupoważnionym osobom,
11. **Zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie swoich danych osobowych,

12. **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.

3. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH:

1. Dane osobowe w jednostce należy:
   a) przetwarzać zgodnie z prawem, rzetelnie i w sposób przejrzysty (zgodność z prawem, rzetelność i przejrzystość),
   b) zbierać w konkretnych, wyraźnych i prawnie uzasadnionych celach (ograniczenie celu),
   c) ograniczać do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych),
   d) uaktualniać w razie potrzeby; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (prawidłowość),
   e) przechowywać w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne (ograniczenie przechowywania),
   f) przetwarzać w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych; w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (integralność i poufność),
2. Dane osobowe w jednostce przetwarzane są zgodnie z prawem, jeżeli:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów np. w celach promocyjnych,
   b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą np. zawieranie umowy o pracę z pracownikami,
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
   d) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
   e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.

3. Dane osobowe szczególnej kategorii przetwarzane są w jednostce zgodnie z prawem, jeżeli:
   a) Osoba, której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie danych osobowych w jednym lub kilku konkretnych celach,
   b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
   c) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
   d) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy,
   e) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi.

4. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH:

Administrator Danych Osobowych:

   a) zobowiązany jest do wdrożenia środków fizycznych, technicznych oraz organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych,
   b) realizuje zasady przetwarzania danych osobowych za które jest odpowiedzialny i potrafi wykazać ich przestrzeganie (rozliczalność),
   c) prowadzi i aktualizuje dokumentacje opisującą sposób przetwarzania danych oraz zapewniającą ochronę danych i bezpieczeństwo ich przetwarzania,
   d) nadaje upoważnienia do przetwarzania danych dla osób przetwarzających jego dane osobowe oraz zapoznaje wszystkich pracowników z niniejszym regulaminem ochrony danych,
   e) organizuje szkolenia z zakresu ochrony danych osobowych dla pracowników oraz innych osób przetwarzających dane,
   f) współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
   g) zgłasza naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadamia osoby, których dane dotyczą o naruszeniu ich danych osobowych, zgodnie z wprowadzonymi procedurami.
   h) wyznacza Inspektora Ochrony Danych Osobowych (IOD) oraz Administratora Systemów Informatycznych (ASI)

5. OBOWIĄZKI INSPEKTORA OCHRONY DANYCH:

1. Administrator Danych Osobowych wyznaczył Inspektora Ochrony Danych Osobowych.

2. Inspektorem Ochrony Danych Osobowych jest Aleksandra Cnota-Mikołajec z którą można skontaktować się za pomocą adresu mailowego: aleksandra@eduodo.pl
3. Inspektor Ochrony Danych Osobowych jest odpowiedzialny w szczególności za:
   a) monitorowanie przestrzegania przepisów dotyczących ochrony danych osobowych oraz niniejszego regulaminu, wykonywanie audytów, sporządzanie raportu po audycie - przynajmniej raz w roku i wydawanie zaleceń,
   b) udzielanie zaleceń co do oceny skutków dla ochrony danych,
   c) opracowuje, nadzoruje i aktualizuje rejestr czynności przetwarzania danych, rejestr kategorii czynności oraz oceny skutków przetwarzania,
   d) współpracę z organami ochrony danych i pełnieniem funkcji punktu kontaktowego dla organów ochrony danych w kwestiach związanych z przetwarzaniem,
   e) przygotowanie oraz aktualizację dokumentacji z zakresu ochrony danych osobowych.

6. NADAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH:

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu upoważnienia do przetwarzania danych osobowych,
2. Przed przystąpieniem do przetwarzania danych osobowych należy zapoznać się z przepisami o ochronie danych osobowych, materiałem informacyjnym dla osób przetwarzających dane osobowe oraz dokumentacją dotyczącą ochrony danych osobowych wprowadzoną przez administratora,
3. Proces nadawania upoważnień do przetwarzania danych osobowych odbywa się w wersji papierowej,
4. Upoważnienia do przetwarzania danych osobowych przygotowuje Inspektor Ochrony Danych,
5. Upoważnienia do przetwarzania danych osobowych akceptuje i podpisuje Administrator Danych Osobowych.
6. Upoważnienie przygotowuje się zgodnie i z odniesieniem do zakresu czynności, jakie wykonuje dana osoba,
7. Upoważnienia do przetwarzania danych osobowych przechowywane są w aktach osobowych danego pracownika oraz w teczce zawierającej dokumentacja dotyczącą ochrony danych osobowych,
8. Upoważnienia do przetwarzania danych osobowych zgodnie z zapisem zawartym w upoważnieniu wygasają z chwilą ustania zatrudnienia lub funkcji.

7. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH:

1. Każda osoba dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a) przetwarzania danych osobowych wyłącznie w zakresie i celach przewidzianych w zadaniach powierzonych przez administratora,
   b) zachowania tajemnicy przetwarzanych danych osobowych w związku z wykonywaniem zadań powierzonych przez administratora,
   c) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   d) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Każda osoba dopuszczona do przetwarzania danych zobowiązuje się do niewykorzystywania danych osobowych w celach niezgodnych z zakresem oraz celem powierzonych zadań,
3. Osobom dopuszczonym do przetwarzania danych osobowych zabrania się przekazywania, bezpośrednio lub przez telefon danych osobowych, osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować,
4. Każda osoba dopuszczona do przetwarzania danych osobowych zapoznaje się z przepisami o ochronie danych osobowych oraz niniejszym regulaminem.

8. ZABEZPIECZENIA DOKUMENTACJI PAPIEROWEJ:

1. Osoby upoważnione do przetwarzania danych odpowiedzialne są za bezpieczeństwo dokumentów i wydruków,
2. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zamykania dokumentów na klucz w szafach, biurkach, sejfach podczas ich nieobecności w pomieszczeniach lub po zakończeniu swojej pracy (tzw. polityka czystego biurka),
3. Pomieszczenia, w których przetwarzane są dane osobowe muszą być każdorazowo zamykane na klucz,
4. Zabrania się pozostawiania kluczy w zamkach drzwi (od wewnątrz i od zewnątrz),
5. Zabrania się pozostawiania kluczy w zamkach szaf i biurek po godzinach pracy lub podczas dłuższej nieobecności pracownika. Klucze należy zabezpieczyć i chować w miejsce niedostępne dla osób nieuprawnionych. Za takie miejsce nie uznaje się pierwszej szuflady w biurku,
6. Osoby upoważnione zobowiązane są do niszczenia dokumentów i tymczasowych wydruków niezwłocznie po ustaniu ich przydatności w niszczarkach,
7. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami np. w korytarzach, pomieszczeniach konferencyjnych,

8. Zabrania się pozostawiania ksero oraz wydruków, zawierających dane osobowe na urządzeniach np. drukarce, kserokopiarce,
9. Zabrania się wywieszania danych osobowych w miejscach widocznych dla osób postronnych; w tym tablicach korkowych,
10. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz np. terenach publicznych, lasach itp.
11. Zabrania się zabierania dokumentów do domu w celu utylizacji ich w prywatnym systemie grzewczym np. piec, kominek.

9. ZASADY WYNOSZENIA DOKUMENTÓW POZA JEDNOSTKĘ:

1. Osoby upoważnione nie mogą wynosić dokumentacji papierowej na zewnątrz jednostki bez pisemnej zgody administratora,
2. Administrator Danych Osobowych zapewnia ewidencjonowanie wydanych pracownikom dokumentów, zawierających dane osobowe,
3. Liczba wynoszonych dokumentów z siedziby administratora jest ograniczona do tego, co niezbędne w stosunku do celów przetwarzania danych osobowych przez pracownika w ramach pracy zdalnej,
4. Osoby upoważnione zobowiązują się do odpowiedniego zabezpieczenia danych osobowych podczas ich wynoszenia np. wynoszenie dokumentów w aktówce. Dokumenty należy przenosić w taki sposób, aby była ona niewidoczna dla osób trzecich,
5. Osoby upoważnione wykonujące pracę w domu zobowiązują się do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy. Przestrzegają zasady czystego biurka oraz zabezpieczają dokumentacje przed wglądem osób nieuprawnionych np. domowników, małżonków.
6. Osoby upoważnione wykonujące pracę w domu zobowiązują się do przechowywania dokumentacji w zamykanych na klucz szafach do których dostęp ma wyłącznie pracownik,
7. Administrator Danych Osobowych korzysta wyłącznie ze sprawdzonych firm kurierskich. W przypadku, gdy dokumenty przewozi pracownik, zobowiązuje się on do zabezpieczania przewożonych dokumentów przed zgubieniem, kradzieżą, zniszczeniem itd.

10. UDOSTĘPNIANIE DANYCH OSOBOWYCH:

1. Administrator zobowiązany jest do prowadzenia rejestru udostępnień danych osobowych,
2. Dane osobowe udostępniane są na pisemny wniosek z uwzględnieniem podstawy prawnej do ich udostępnienia, chyba, że przepis innej ustawy stanowi inaczej,

3. Wniosek o udostępnienie danych musi zawierać:
   a) nazwę jednostki organizacyjnej lub imię i nazwisko osoby, której udostępniane są dane,
   b) termin, podstawę prawną oraz zakres udostępnianych danych,
4. Wnioski o udostępnienie danych osobowych mogą być przyjmowane przez każdą osobę upoważnioną,
5. Każdy otrzymany wniosek o udostępnienie danych należy przekazać administratorowi lub inspektorowi ochrony danych osobowych.

11. POWIERZENIE DANYCH OSOBOWYCH:

1. Administrator Danych Osobowych korzysta z usług podmiotu przetwarzającego, który zapewnia wystarczającą gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych i zapewnia ochronę praw osób, których dane przetwarza,
2. Powierzenie przetwarzania danych osobowych może nastąpić wyłącznie poprzez podpisanie umowy powierzenia przetwarzania danych,
3. Umowa powierzenia przetwarzania danych zawiera:
   a) przedmiot i czas trwania przetwarzania,
   b) charakter i cel przetwarzania,
   c) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
   d) obowiązki podmiotu przetwarzającego i prawa administratora.
4. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora i zapewnia, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy,
5. Podmiot przetwarzający ma zapewnić wszelkie środki wymagane zgodnie z art. 32 RODO,
6. Po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora, podmiot przetwarzający usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszystkie istniejące kopie,
7. Podmiot przetwarzający umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzenie audytów.

12. ZABEZPIECZENIE SPRZĘTU IT ORAZ NOŚNIKÓW ZEWNĘTRZNYCH:

1. Użytkownik zobowiązany jest do ochrony sprzętu IT przed jakimkolwiek zniszczeniem lub uszkodzeniem. Sprzętem IT jest: komputer stacjonarny, laptop, monitor, drukarka, skaner, tablet, smartfon i nośniki zewnętrzne, którymi są: dyski twarde, płyty CD/DVD, pendrive, pamięć typu „flash" itp.

2. Każdy użytkownik zobowiązany jest do natychmiastowego zgłoszenia zagubienia, utraty, awarii lub zniszczenia powierzonego mu sprzętu IT,
3. Zabrania się samodzielnego demontażu sprzętu IT, instalowania dodatkowych urządzeń np. twardych dysków, instalowania oprogramowania bez wiedzy administratora lub podłączenia jakichkolwiek niezatwierdzonych przez administratora urządzeń np. smartfonów, pendrive do systemu informatycznego,
4. Zabrania się umożliwiania osobom nieuprawnionym wglądu do danych wyświetlanych na monitorach komputerowych.
5. Monitory komputerów oraz laptopów muszą być odwrócone w sposób uniemożliwiający wgląd osobom nieupoważnionym. Jeżeli istnieje taka konieczność należy zabezpieczyć monitor filtrem prywatyzującym,
6. Zabrania się dopuszczania osób nieupoważnionych do sprzętu IT,
7. Przed odejściem od stanowiska pracy, użytkownik zobowiązany jest do każdorazowego blokowania hasłem komputera (skrót klawiszowy: WINDOWS+L) oraz wylogowania się ze wszystkich programów, w których przetwarzane są dane osobowe,
8. Po zakończeniu pracy użytkownik zobowiązuje się do wylogowania się z systemu informatycznego oraz wyłączenia sprzętu komputerowego,
9. Nośniki danych są przechowywane w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym oraz w miejscu zabezpieczającym przed zagrożeniami tj. zalanie, pożar, wpływ pól elektromagnetycznych,
10. Użytkownicy zobowiązani są do niezwłocznego i trwałego usuwania danych osobowych z nośników zewnętrznych po ustaniu powodu ich przechowywania, chyba, że przepisy odrębne stanowią inaczej,
11. Użytkownicy zobowiązani są do niezwłocznego i trwałego usuwania plików z nośników zewnętrznych do których mają także dostęp nieupoważnieni użytkownicy.

13. NISZCZENIE NOŚNIKÓW ZEWNĘTRZNYCH:

1. Niszczenie nośników zewnętrznych oznacza takie uszkodzenie mechaniczne, które uniemożliwia odzysk zapisanych na nich informacji,
2. Niszczeniu podlegają nośniki zewnętrzne dla których minął okres ich ważności, nie przewiduje się ich dalszego użytkowania (chyba, że przepisy odrębne stanowią inaczej) lub istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać przechowywania informacji,
3. Niszczenie nośników zewnętrznych odbywa się na polecenie Administratora Danych Osobowych oraz za wiedzą Inspektora Ochrony Danych Osobowych,

4. Niszczenie odbywa się za pomocą firmy zewnętrznej spełniającej standardy ISO/IEC 21964 oraz DIN 66399.
5. Po zakończeniu niszczenia sporządzony zostaje rejestr likwidacji nośników.

14. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ:

1. Przesyłanie danych osobowych za pomocą poczty elektronicznej może odbywać się tylko przez osoby upoważnione,
2. Przesyłając dane osobowe należy wykorzystywać mechanizmy kryptograficzne,
3. Hasło zabezpieczające wysyłane pliki musi się składać się z minimum osiem znaków; w tym duże i małe litery, oraz cyfry lub znaki specjalne. Hasło należy przesłać inną metodą np. telefonicznie. Zabrania się przesyłania hasła na ten sam adres e-mail,
4. Użytkownicy zobowiązani są do zwracania szczególnej uwagi na poprawność adresu odbiorcy dokumentu. Zaleca się, aby w treści wysyłanej wiadomości zawrzeć prośbę o potwierdzenie otrzymania maila,
5. Zabrania się otwierania plików (załączników) bez weryfikacji nadawcy. Tego typu maile mogą zawierać załączniki ze szkodliwym oprogramowaniem, które infekują komputer użytkownika, czego skutkiem jest utrata danych osobowych,
6. Zabrania się otwierania linków w mailach bez weryfikacji nadawcy, gdyż mogą to być odnośniki do stron zainfekowanych lub niebezpiecznych. Wchodząc na tego typu linki użytkownik infekuje komputer oraz pozostałe komputery w sieci,
7. Każdy przypadek wykrycia podejrzanych wiadomości należy zgłosić administratorowi i inspektorowi ochrony danych osobowych,
8. Użytkownikom nie wolno rozsyłać maili niezwiązanych z pracą w formie „łańcuszków szczęścia",
9. Wysyłając maile do wielu adresatów należy użyć opcji „ukryta kopia". Zabrania się rozsyłania wiadomości do wielu adresatów z użyciem „do wiadomości",
10. Użytkownicy muszą kasować niepotrzebne maila minimum raz w miesiącu,
11. Zabrania się używania danych osobowych lub poufnych informacji w temacie wiadomości,
12. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
13. Zabrania się uruchamiania przekierowania wiadomości ze służbowej skrzynki mailowej na prywatną,
14. Użytkownicy korzystający z maila zobowiązani są do przestrzegania prawa własności przemysłowej i prawa autorskiego,
15. Zabrania się korzystania z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania,

16. Użytkownik bez zgody administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe administratora; jego pracowników, klientów, dostawców, kontrahentów za pośrednictwem Internetu; w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
17. Użytkownicy nie wykorzystują komunikatorów dostępnych w sieciach oraz usługach społecznościowych w celach służbowych,
18. Każdy użytkownik jest odpowiedzialny za tekstową, dźwiękową lub graficzną treść wysyłanych wiadomości.

15. KORZYSTANIE Z INTERNETU:

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych,
2. Zabrania się zgrywania na dysk twardy komputera, instalowania oraz uruchamiania programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki można pobrać wyłącznie za zgodą ADO i tylko w uzasadnionych przypadkach,
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu,
4. Zabrania się wchodzenia na strony internetowe, które prezentują informacje o charakterze przestępczym, pornograficznym, innym zakazanym przez prawo, gdyż na większości tych stron jest zainstalowane szkodliwe oprogramowanie, które w sposób automatyczny infekuje system operacyjny komputera,
5. Zabrania się włączania opcji autouzupełniania formularzy i zapamiętywania haseł w przeglądarce,
6. Podczas korzystania z zaszyfrowanego przez przeglądarkę połączenia, każdy użytkownik zobowiązany jest do sprawdzenia czy połączenie jest zabezpieczone. Należy zwrócić uwagę na ikonę kłódki oraz adresu internetowego rozpoczynającego się od „https". Dla pewności należy kliknąć ikonę kłódki, aby sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel,
7. Użytkownicy muszą zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę internetową np. banku, e-sklepu, poczty mailowej, a także w przypadku podania loginów, haseł, PIN-ów, numerów kart płatniczych za pomocą Internetu. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank,
8. Użytkownicy mogą korzystać z Internetu w celach prywatnych wyłącznie okazjonalnie i za zgodą administratora. Korzystanie z Internetu w celach prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne

wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego administratora,

9. Użytkownicy korzystający z Internetu zobowiązani są do przestrzegania prawa własności przemysłowej i prawa autorskiego,
10. Administrator Danych Osobowych zastrzega sobie prawo do kontrolowania sposobu korzystania przez użytkownika z komputera w zakresie dozwolonym przepisami prawa oraz regulacjami wewnętrznymi,
11. Administrator Danych Osobowych zastrzega sobie prawo do kontrolowania czasu spędzonego przez użytkownika w Internecie w uzasadnionym zakresie,
12. Administrator Danych Osobowych ma prawo blokować dostęp do niektórych treści dostępnych w Internecie.

16. NADAWANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM:

1. Każdy użytkownik dopuszczony do przetwarzania danych w systemie informatycznym musi zapoznać się z regulaminem ochrony danych oraz przepisami o ochronie danych,
2. Każdy użytkownik mający dostęp do danych osobowych w systemie informatycznym np. na dysku sieciowym, programie oraz poczcie elektronicznej musi posiadać własny identyfikator (login) do logowania się. Wyjątek stanowi konto użytkownika w systemie Windows,
3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji,
4. ADO ustala niepowtarzalny identyfikator i hasło dla każdego użytkownika. Nadany login oraz pierwsze hasło podawane są w formie ustnej,
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie,
6. W przypadku utraty przez daną osobę uprawnień dostępu do danych w systemie informatycznym należy niezwłocznie wyrejestrować identyfikator z systemu lub zablokować, unieważnić hasło oraz podjąć inne stosowne działania celem zapobieżenia dalszemu dostępowi tej osoby do danych,
7. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień np. przydzielenia sobie uprawnień administratora w systemie, tworzenia kont gościa itd.,
8. Użytkownicy zobowiązani są do pracy na własnym koncie. Zabronione jest umożliwianie pracy na koncie i przekazywanie danych dostępowych w postaci loginu oraz hasła innym użytkownikom.

17. POLITYKA HASEŁ:

1. Hasła nie mogą być powszechnie używanymi słowami. Zabrania się wykorzystywania dat narodzin, ślubu oraz innych ważnych wydarzeń, imion i nazwisk osób bliskich, imion zwierząt, popularnych słów, typowych zestawów np. 123,
2. Użytkownik zobowiązuje się do zachowania hasła w poufności; nawet po utracie jego nieważności.
3. Hasła nie mogą być ujawniane innym osobom. Zabrania się zapisywania haseł na kartkach i w notesach, naklejania ich na komputerze lub tablicy korkowej, trzymania w szufladzie lub pod klawiaturą,
4. Zapisane hasło musi być przechowywane w zamkniętej kopercie w sejfie,
5. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany hasła, gdy zostało ono ujawnione,
6. Użytkownik zobowiązany jest do zmiany swojego hasła (nie rzadziej niż co 30 dni),
7. Użytkownik zobowiązany jest do samodzielnej zmiany hasła, jeżeli system tego nie wymusza,
8. Administrator zobowiązany jest do ustawienia zmiany hasła, jeżeli system mu to umożliwia,
9. Hasło użytkownika składa się z minimum ośmiu znaków; w tym duże i małe litery, cyfry i znaki specjalne.

18. OCHRONA ANTYWIRUSOWA:

1. Administrator Danych Osobowych zobowiązany jest do instalacji oprogramowania antywirusowego; w tym zapewnienia odpowiedniej ilości licencji na każdym komputerze,
2. System antywirusowy zapewnia ochronę systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej,
3. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada,
4. Zabrania się wyłączania systemu antywirusowego podczas pracy systemu informatycznego, przetwarzającego dane osobowe,
5. Użytkownik zobowiązany jest do niezwłocznego poinformowania administratora i inspektora ochrony danych osobowych, administratora sieci informatycznych w przypadku stwierdzenia zainfekowania systemu lub pojawiania się komunikatu o treści ,,Twój system jest zainfekowany!" Wykryto zagrożenie",
6. Aktualizacja definicji wirusów odbywa się automatycznie przez system - codziennie.

19. NAPRAWA I PRZEGLĄD SIECI I SPRZĘTU KOMPUTEROWEGO:

1. Naprawa sieci oraz sprzętu komputerowego następuje za zgodą Administratora Danych Osobowych pod nadzorem upoważnionego przez niego pracownika,
2. Umowy dotyczące instalacji, naprawy i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi,
3. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu,
4. Zabrania się podłączania do gniazdek elektrycznych sieci komputerowych czajników, grzałek i innych urządzeń elektrycznych, które nie są sprzętem komputerowym, aby zapewnić jak najbardziej bezawaryjną i bezpieczną pracę w sieci komputerowej,
5. Należy zwracać szczególną uwagę na ewentualne luźne kable sieciowe tzn. nie deptać ich, nie zginać, nie stawiać na nich krzeseł itp.,
6. Każdy komputer pracujący w sieci komputerowej powinien być wyposażony w zasilacz awaryjny tzw. UPS.

20. ZASADY POSTĘPOWANIA W SYTUACJACH NARUSZENIA:

1. Wszystkie osoby upoważnione zobowiązane są do niezwłocznego powiadomienia administratora oraz inspektora ochrony danych osobowych o fakcie wystąpienia naruszenia,
2. Przed przystąpieniem do pracy, osoby upoważnione zobowiązane są do dokonania oceny i oględzin miejsca ich pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań, związanych z ochroną danych osobowych,
3. Do sytuacji wymagających powiadomienia należą:
   a) niewłaściwie zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
4. Do incydentów wymagających powiadomienia należą:
   a) Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),

c) Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

5. Typowe przykłady incydentów wymagające reakcji:
   a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b) dokumentacja jest niszczona bez użycia niszczarki,
   c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
   f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia administratora,
   g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
   h) telefoniczne próby wyłudzenia danych osobowych,
   i) kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi,
   j) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   l) hasła do systemów przyklejone są w pobliżu komputera.

21. DODATKOWE DOKUMENTY:

Jako załączniki do regulaminu zostaną wprowadzone następujące dokumenty określające:

a) Wykaz miejsc przetwarzania danych osobowych,
b) Wykaz danych przetwarzanych przez administratora,
c) Wykaz zabezpieczeń stosowanych przez administratora.

22. ZAPISY KOŃCOWE:

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy,
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez administratora lub inspektora za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r,

3. Z naruszenia obowiązków wynikających z niniejszego dokumentu lub z postępowania sprzecznego mogą zostać wyciągnięte konsekwencje dyscyplinarne w postaci pisemnego upomnienia, nagany lub kary finansowej. Do wyciągania konsekwencji prawo ma administrator danych osobowych.

Aleksandra Cnota-Mikołajec
Inspektor Ochrony Danych

.....
Inspektor Ochrony Danych

DYREKTOR
Powiatowego Domu Kultury
w Raciborzu
Robert Myśliwy

.....
Administrator Danych Osobowych