Załącznik nr 1 do zarządzenia
Burmistrza Miasta nr B.120.1.28.2020
z dnia 11 maja 2020r.

Polityka Ochrony Danych Osobowych Urzędu Miejskiego w Kuźni Raciborskiej

Spis treści

Wprowadzenie

Niniejsza Polityka Ochrony Danych Osobowych została stworzona w związku z wymaganiami jakie stawia przed Administratorami danych osobowych oraz Podmiotami przetwarzającymi 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 - (Dz. Urz. UE L 119, s. 1), zwane dalej RODO oraz ustawa z dnia 10 maja 2018 r . o ochronie danych osobowych wraz z wydanymi na jej podstawie aktami wykonawczymi.

Niniejszy dokument dotyczy wszystkich przetwarzanych przez Urząd Miejski danych osobowych, niezależnie od formy ich przetwarzania (tradycyjnej lub w systemach informatycznych).

Definicje

Polityka Ochrony Danych Osobowych (Polityka) – niniejsza Polityka, o ile z kontekstu nie wynika inaczej.

Dane Osobowe – są to dane o zidentyfikowanej, bądź możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą).

Dane osobowe szczególnej kategorii - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Administrator Danych Osobowych („Administrator") - jest decydentem w procesie przetwarzania danych osobowych. Decyduje o sposobie i celu przetwarzania danych.

Inspektor Ochrony Danych Osobowych (IOD) – to osoba powołana przez Administratora celem informowania o obowiązkach wynikających z przepisów prawa o ochronie danych osobowych, w tym RODO, nadzoru nad przestrzeganiem tych przepisów, zarządzania ryzykiem, współpracy z organami nadzorczymi oraz osobami, których dane dotyczą.

Administrator Systemu (ASI) - pracownik na stanowisku inspektora ds. obsługi informatycznej, zarządza systemami informatycznymi Urzędu Miejskiego w Kuźni Raciborskiej.

RODO (Rozporządzenie) – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

§ 1. Obowiązek zapoznania pracowników z Polityką Bezpieczeństwa

Pracownicy mający dostęp do danych osobowych przetwarzanych w Urzędzie Miejskim w Kuźni Raciborskiej są zobowiązani do zapoznania się z niniejszą Polityką.

§ 2

Podstawy przetwarzania

1. Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach gdy spełniony jest co najmniej jeden z warunków przetwarzania przewidzianych w RODO (art 6, art. 9, art. 10 RODO), w związku z realizacją przepisów prawa powszechnie obowiązującego.
2. W przypadku wątpliwości co do wyboru podstawy prawnej pracownicy zasięgają opinii Inspektora Ochrony Danych (IOD).

§ 3

Powierzenie przetwarzania danych osobowych

1. Administratorowi celem realizacji zadań pracodawcy, własnych i zleconych (powierzonych) oraz organu administracji publicznej może przekazać dane osobowe innym osobom fizycznym lub podmiotom do przetwarzania.
2. Administrator dla realizacji powyższych zadań przekazuje dane osobowe tylko na podstawie umowy lub innego instrumentu prawnego.
3. Zlecanie jakichkolwiek czynności, związanych z przetwarzaniem danych osobowych podmiotom zewnętrznym w imieniu Administratora na podstawie umowy lub innego instrumentu prawnego jest formą powierzenia przetwarzania danych osobowych.
4. Przetwarzanie przez podmiot przetwarzający danych osobowych może wystąpić w przypadku:
   1) przekazania do realizacji zadań Administratorowi innemu podmiotowi;
   2) outsourcingu usług zewnętrznych;
   3) zawierania umów cywilnoprawnych (usług i zlecenia);
5. Administrator przed powierzeniem sprawdza, czy korzysta wyłącznie z usług takich podmiotów przetwarzających, które:
   1) gwarantują wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą;
   2) korzystają z usług innego podmiotu przetwarzającego tylko na podstawie szczegółowej lub zgody pisemnej Administratora;
   3) informują w przypadku pisemnej zgody o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym ADO możliwość wyrażenia sprzeciwu wobec takich zmian.

6. Decyzję o powierzeniu przetwarzania danych osobowych na podstawie umowy lub innego instrumentu prawnego podejmuje Administrator.
7. Inspektor Ochrony Danych we współpracy z pracownikiem merytorycznym przygotowuje umowę lub inny instrument prawny, które powinny precyzyjnie określać szeroko rozumiane okoliczności powierzenia oraz zawierać elementy wymienione w art. 28 RODO, szczegółowe deklaracje, co do obowiązków podmiotu przetwarzającego.

§ 4
Udostępnienie danych osobowych

1. W przypadkach określonych w prawie, udostępnienie danych osobowych przez ADO może odbywać się także na podstawie wniosku (w tym oświadczenia) podmiotu upoważnionego o udostępnienie danych.

2. Wniosek musi zawierać cel przetwarzania i podstawę prawną oraz gwarancje odbiorcy wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych, by przetwarzanie udostępnionych danych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

§ 5
Realizowanie obowiązków informacyjnych

1. W celu zapewnienia rzetelności i przejrzystości przetwarzania danych osobowych podczas ich pozyskiwania Administrator, przy pomocy pracowników, udziela na piśmie lub w inny sposób, w tym elektronicznie wszelkich informacji w sprawie przetwarzania zgodnie z art. 12 RODO, KPA oraz innych przepisów mających zastosowanie.
2. Pracownik merytoryczny przygotowuje informację o przetwarzaniu danych w zakresie danych które przetwarza i realizuje obowiązek informacyjny. Obowiązek informacyjny konsultowany jest z Inspektorem Ochrony Danych.
3. Obowiązek informacyjny realizuje się poprzez:
   1) umieszczenie informacji o przetwarzaniu danych w Biuletynie Informacji Publicznej Urzędu oraz na stronie internetowej Urzędu Miejskiego;
   2) wywieszeniu informacji o przetwarzaniu danych we wszystkich lokalizacjach Urzędu Miejskiego na tablicach ogłoszeń,
   3) wyłożeniu lub wywieszeniu informacji o przetwarzaniu danych w formie ulotek lub wywieszek w miejscach wyznaczonych do pisania podań lub wniosków albo w biurze;
   4) umieszczeniu informacji o przetwarzaniu danych (odrębnie) na formularzu;
   5) umieszczeniu informacji o przetwarzaniu danych (odrębnie) na wzorach wniosków, podań, zawiadomień stron itp. jeśli wynika taki obowiązek lub potrzeba;
   6) wpisaniu do umów brakujących informacji z informacji o przetwarzaniu danych.

§ 6
Prawa osoby, które dane dotyczą

Realizacja praw osób, których danych dotyczą zostanie opracowana w oddzielnych procedurach

§ 7
Rejestr czynności przetwarzania danych osobowych

1. Administrator Danych prowadzi Rejestr Czynności Przetwarzania Danych oraz Rejestr Kategorii Czynności Przetwarzania, w których inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
2. Rejestry stanowią narzędzie rozliczania przestrzeganie przepisów i wskazuje ich przestrzeganie zgodnie z RODO i UODO w Urzędzie.
3. Rejestry prowadzi Inspektor Ochrony Danych przy pomocy sekretarza.
4. Wniosek o wpisanie w ewidencjach i rejestrach, a także ich aktualizację składają Kierownicy Referatów.

§ 8
Analiza ryzyka

1. IOD wykonuje analizę ryzyka przetwarzania danych. Inspektor dokonuje wyboru metodologii, uwzględniając zalecenia Prezesa Urzędu Ochrony Danych Osobowych.

2. Wyznaczona osoba dokonuje przeglądu analizy ryzyka regularnie, co najmniej 1 raz w roku i powiadamia Administratora o wynikach tej oceny. W przypadku istotnej zmiany u Administratora organizacyjnej, strukturalnej, technicznej, technologicznej i odnoszącej się do Danych osobowych, Administrator poleca Wyznaczonej osobie przeprowadzenie aktualnej analizy ryzyka naruszenia praw lub wolności osób.

3. Administrator przechowuje dokumentację z analizy ryzyka wykonywanej przez ostatnie 5 pełnych lat kalendarzowych.

4. Administrator uwzględnia wyniki analizy ryzyka w projektowaniu lub zmianach w obrębie poszczególnych procesów przetwarzania Danych osobowych.

§ 9
Zabezpieczenie danych osobowych

Administrator Danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych jednostki, a w szczególności: środków określonych w § 14 oraz innych dokumentach dotyczących zabezpieczeń.

§ 10
Zalecane sposoby zabezpieczania danych

1. **Zaleca się stosowanie następujących środków zabezpieczenia danych osobowych przetwarzanych w formie tradycyjnej (papierowej):**
    1) dokumenty z danymi osobowymi winny zostać pozbawione danych osobowych zawartych na obwolutach;
    2) przenoszenie dokumentów z danymi osobowymi winno następować w aktówkach, teczkach lub w inny sposób, uniemożliwiający podgląd danych;
    3) zabronione jest pozostawianie danych osobowych bez nadzoru (np. w samochodzie, domu);
    4) zabronione jest korzystanie z danych osobowych w miejscach publicznych (np. kawiarniach, komunikacji miejskiej);
    5) dane osobowe poza obszarem przetwarzania winny być zabezpieczone przed osobami nieupoważnionymi w zamykanych na klucz szafkach, sejfach lub pomieszczeniach.

2. Zaleca się stosowanie następujących środków zabezpieczenia danych osobowych przetwarzanych w formie elektronicznej:

1) zabezpieczenie nośników danych poprzez zaszyfrowanie danych;
2) nie przenoszenie/przesyłanie zaszyfrowanego nośnika danych wraz z kluczem do jego odszyfrowania;
3) hasła dostępowe zgodne z Polityką Haseł obowiązującą w Urzędzie;
4) niepozostawianie nośników danych osobowych bez nadzoru (np. w samochodzie, domu);
5) niekorzystanie z danych osobowych w miejscach publicznych (np. kawiarniach, komunikacji miejskiej);
6) niepodłączanie służbowego sprzętu do ogólnodostępnych, niezabezpieczonych sieci wifi;
7) korzystanie wyłącznie z komputerów zabezpieczonych antywirusem i firewallem;
8) korzystanie wyłącznie z komputerów zabezpieczonych procesem uwierzytelnienia;
9) zabezpieczenie nośników danych osobowych poza obszarem przetwarzania danych osobowych przed osobami nieupoważnionymi w zamykanych na klucz szafkach, sejfach lub pomieszczeniach.

3 . Zaleca się niszczenie wydruków i zapisów na nośnikach danych:

1) Nośniki danych (magnetyczne, optyczne, flash i inne) przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
2) Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji, wielokrotne ich nadpisywanie oraz formatowanie nośnika.

3) Poprawność przygotowania nośnika danych powinna być sprawdzona przez ASI.
4) Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie, itp.
5) Wydruki, po wykorzystaniu, należy zniszczyć w mechanicznej niszczarce do papieru.

§ 11

Zdarzenia naruszające ochronę danych osobowych

Za naruszenie lub próbę naruszenia zasad przetwarzania danych osobowych uznaje się:

1) nieodpowiednie zabezpieczenie pomieszczeń, urządzeń lub dokumentów;
2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
3) naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe;
4) uszkodzenie, utratę, zmianę, lub nieuprawnione kopiowanie danych osobowych;
5) udostępnienie lub możliwość udostępnienia danych osobowych osobom nieuprawnionym;
6) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczeń;
7) przetwarzanie danych osobowych bez upoważnienia;
8) przetwarzanie danych osobowych niezgodnie z ich zakresem lub celem zebrania;
9) przetwarzanie danych osobowych poza obszarem przetwarzania danych osobowych bez wiedzy i zgody Administratora;
10) naruszenie praw osób, których dane dotyczą;
11) niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie na klucz pomieszczeń, szaf, biurek.

§ 12

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Naruszenie bezpieczeństwa danych osobowych występuje w przypadku naruszenia bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. W przypadku stwierdzenia naruszenia, bądź możliwości zaistnienia naruszenia, każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana powiadomić niezwłocznie o tym fakcie Administratora, IOD lub ASI (w przypadku incydentów dotyczących infrastruktury IT).

2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora,

IOD lub ASI, należy:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców;
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku;
7) udokumentować wstępnie zaistniałe naruszenie;
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby upoważnionej.

3. Każdorazowo po otrzymaniu informacji o zaistnieniu lub możliwości zaistnienia naruszenia zasad ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło spowodować ryzyko naruszenia praw lub wolności osoby fizycznej, której dane dotyczą. Czynności te ujęte są w raporcie z naruszenia bezpieczeństwa zasad ochrony danych osobowych. W przypadku stwierdzenia wystąpienia naruszenia ochrony danych osobowych, stosownie do przepisów dokonuje zgłoszenie do Prezesa Urzędu Ochrony Danych osobowych lub informuje podmiot uprawniony.

4. 1. Administrator oraz IOD prowadzi postępowanie wyjaśniające w toku, którego:

1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
2) proponuje ewentualne działania zaradcze;
3) zaleca szereg działań mających na celu przywrócenia prawidłowego działania organizacji po wystąpieniu incydentu;
4) rekomenduje działania mające na celu zapobieganie podobnym incydentom w przyszłości lub zmniejszenie strat w momencie ich zaistnienia;
5) prowadzi ewidencję naruszeń ochrony danych osobowych.

2. W ewidencję naruszeń ochrony danych osobowych wpisuje się wszystkie naruszenia, które podlegają lub nie podlegają zgłoszeniu do organu nadzorczego.

3. Jakiekolwiek próby powstrzymania osoby uprawnionej lub pracownika przed zgłoszeniem naruszenia lub podejrzenia naruszenia bezpieczeństwa danych są zabronione mogą powodować konsekwencje dyscyplinarne lub karne w stosunku do osób podejmujących takie działanie.
4. Podobnym konsekwencjom podlegają próby karania osób uprawnionych lub pracowników za zgłoszenie naruszenia lub podejrzenia naruszenia.
5. Administrator chroni wszystkie osoby uprawnione lub pracowników zgłaszających w dobrej wierze podejrzenia zagrożenia lub naruszenia bezpieczeństwa danych, niezależnie od zasadności tych podejrzeń.

§ 13
Zgłaszanie naruszeń

1. Administrator Danych po zgłoszeniu naruszenia ochrony danych osobowych bada czy naruszenie wystąpiło.
2. W przypadku stwierdzenia naruszenia IOD przeprowadza ocenę naruszenia pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych.
3. Administrator Danych w przypadku stwierdzenia naruszenia bezpieczeństwa, które nie występuje ryzyko naruszenia praw i wolności osób fizycznych lub jest to mało prawdopodobne, nie zgłasza naruszenie organowi nadzoru a naruszenie wpisuje się do prowadzonej ewidencji naruszeń.

3, W przypadku stwierdzenia naruszenia bezpieczeństwa i gdy występuje ryzyko naruszenia praw i wolności osób fizycznych, Administrator Danych:

1) zgłasza naruszenie organowi nadzorczemu;
2) powiadamia osoby, której dane dotyczą o naruszeniu;

4. Administrator Danych w przypadku stwierdzenia naruszenia podejmuje działania mające na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.
5. Ewidencje naruszeń i związaną z tym dokumentację prowadzi sekretarz.

§ 14
Wykorzystywane środki zabezpieczenia danych

1. **Do zastosowanych środków technicznych należy:**
    1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej;
    2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1;
    3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu;
    4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa

dokumentacji.

2. **Do zastosowanych środków organizacyjnych należy:**
    1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych;
    2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;
    3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę;
    4) kontrolowanie, aby do pomieszczenia serwerowni, w której następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami. Dostęp ten jest kontrolowany za pomocą drzwi połączonymi z systemem kontroli dostępu;
    5) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez ASI, zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego;
    6) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ochrony danych osobowych lub być uwzględnione na liście osób przeszkolonych;
    7) stosownie do wymagań przepisów prawa europejskiego i polskiego pracownicy dostają upoważnienie do przetwarzania danych osobowych;
    8) podłączenie danego użytkownika do sieci komputerowej dokonuje ASI.
3. **Do zastosowanych środków ochrony informatycznej należą:**
    1) ochrona przed utratą zgromadzonych danych przez wykonywanie kopii zapasowych na odrębnych nośnikach oraz zewnętrznych serwerach backup, z których w przypadku awarii odtwarzane są dane;
    2) ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych. Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu;
    3) wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie, oddzielone od szkieletu sieci komputerowej;
    4) aby uzyskać, zmodyfikować lub usunąć prawa dostępu do zasobów sieci

informatycznej, kierownik referatu zwraca się do ASI z odpowiednim wnioskiem, w którym zawarte będą dane użytkownika oraz uprawnienia, jakie ma on mieć nadane;

5) w systemie informatycznym jednostki zastosowano autoryzację użytkownika w oparciu o Active Directory;
6) zastosowano firewall, który ma za zadanie uwierzytelnianie źródła informacji przychodzących oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Firewall składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez Śląskie Centrum Społeczeństwa Informacyjnego;
7) firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku;
8) oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów;
9) w pomieszczeniach, w których znajdują się serwery zamontowane są czujniki temperatury, wilgotności powietrza oraz zaniku zasilania;
10) w pomieszczeniach w których znajdują się serwery zamontowana jest klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza;
11) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę oraz czujka ruchu;
12) większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych;
13) dla potrzeb systemu informatycznego w jednostce stosowane jest zabezpieczenie antywirusowe i ochrona sieci, w zakres ochrony wchodzi:
    1. ochrona poczty;
    2. skanowanie ruchu internetowego;
    3. ochrona systemów plików;
    4. kontrola zmian w systemie plików;
    5. monitorowanie procesów w pamięci;
    6. monitorowanie zmian w rejestrze systemowym;
    7. przywracanie systemu.

§ 15
Monitorowanie zabezpieczeń

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem

czynności:

1) Administrator danych osobowych (lub osoba przez niego wyznaczona);
2) Inspektor Ochrony Danych;
3) ASI.

2. W ramach kontroli należy zwracać szczególna uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych;
   b) przestrzeganie przepisów dotyczących ochrony danych osobowych;
   c) kontrolę ewidencji nośników danych;
   d) kontrolę właściwej częstotliwości zmiany haseł;
   e) spełnianie obowiązków informacyjnych RODO.

§ 16
Zasady prowadzenia ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych

1. Administrator danych prowadzi ewidencję wszystkich pracowników jednostki zatrudnionych przy przetwarzaniu danych osobowych i posiadających odpowiednie upoważnienia.
3. Jakakolwiek zmiana informacji wyszczególnionej w ewidencji wymaga natychmiastowego poinformowania administratora danych.
4. Za zgłaszanie zmian zawartych w ewidencji odpowiedzialny jest bezpośredni przełożony pracownika.

§ 17
Dostęp do danych osobowych

1. Realizacja dostępu do danych osobowych przetwarzanych przez administratora jest jednoznaczna z tym, że Administrator wydaje polecenie przetwarzania danych osobowych, a osoby fizyczne lub podmioty oświadczają, że przyjmuje te polecenie do realizacji zgodnie z wydanym poleceniem.
2. Warunki dostępu określa upoważnienie, umowa lub inny instrument prawny.
3. Wydane upoważnienie, zawarta umowa lub inny instrument prawny jest poleceniem wydanym przez administratora do przetwarzania danych osobowych w zakresie określonym przez upoważnienie, umowę lub inny instrument prawny.
4. Dostęp do danych osobowych i systemu informatycznego uzyskują osoby i podmioty uprawnione w godzinach pracy Urzędu. Administrator może zezwolić na dostęp po godzinach pracy.
5. Dostęp do zbiorów danych osobowych przetwarzanych w Urzędzie uzyskują pracownicy Urzędu oraz strony trzecie po:

1) przeszkoleniu z zakresu bezpiecznego przetwarzania danych osobowych i zapoznaniu się obowiązującymi w tym zakresie przepisami prawa;
2) podpisaniu oświadczenia o zachowaniu w poufności informacji związanych z bezpieczeństwem danych, systemów informatycznych i ich zabezpieczeniem, naruszeń bezpieczeństwa z którymi się zapoznał, uzyskanych w związku z wykonywaną pracą lub realizacją umowy i nie ujawniania tych informacji w czasie trwania zatrudnienia lub umowy jak i po ich rozwiązaniu oraz zgłoszenia wszystkich naruszeń ochrony danych osobowych;
3) wydaniu imiennego upoważnienia do przetwarzania danych osobowych, które określa zakres i uprawnienia do dostępu i przetwarzania danych;
4) w zakresie określonym przez umowę lub inny instrument prawny.

6. Upoważnienie, umowa lub inny instrument prawny musi określać uprawnienia osób lub podmiotów do dostępu do danych osobowych, zasobów i obszaru bezpiecznego i ich przetwarzania. Zakres uprawnień określa także dostęp do systemu tradycyjnego i informatycznego.
7. Upoważnienia do przetwarzania danych osobowych podpisuje Administrator lub z upoważnienia Sekretarz.
8. Upoważnienie wydaje inspektor ds. kadrowych w momencie zatrudnienia nowego pracownia po uprzednim uzgodnieniu go z Kierownikiem Referatu.
9. Administrator prowadzi Rejestr wydanych upoważnień w którym prowadzi się ewidencję osób upoważnionych. Wpisy do rejestru dokonuje się na podstawie wniosku lub zawartej umowy.
10. Rejestr może być prowadzony odrębnie dla pracowników dla pozostałych osób.

§ 18
Upoważnienie do przetwarzania danych osobowych

1. Do nadawania i anulowania upoważnień do przetwarzania danych osobowych zarówno w zbiorach papierowych jak i w systemach informatycznych uprawniony jest wyłącznie Administrator danych osobowych lub osoba przez niego wyznaczona. Dane osobowe mogą być przetwarzane wyłącznie na jego polecenie bądź na podstawie przepisów obowiązującego prawa.
2. Upoważnienie wydane może być na czas określony lub do odwołania.
3. Upoważnienia określają zakres danych osobowych, które dany pracownik przetwarza
4. Upoważnienie wydawane jest jedynie w zakresie niezbędnym do wykonywania powierzonych przez Administratora czynności przetwarzania danych osobowych.
5. Zmiana zakresu upoważnienie wymaga ponownego nadania upoważnienie.
6. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,

służących do zbierania lub przetwarzania danych osobowych, mogą być dopuszczeni wyłącznie pracownicy posiadający aktualne, ważne upoważnienia.

7. Administrator danych zapoznaje pracowników z przepisami o ochronie danych osobowych.

§ 19
Odpowiedzialność pracownika

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Przekazywanie informacji o występujących zagrożeniach lub naruszeniach poza Urzędem jest zabronione, a zwłaszcza w zakresie dotyczącym systemu informatycznego.
3. Naruszenie przepisów niniejszej polityki może powodować konsekwencje dyscyplinarne lub inne sankcje w stosunku do osób podejmujących takie działanie.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomi o tym fakcie odpowiedniej osoby.

§ 20
Dokumentacja przetwarzania prowadzona przez ADO

l. ADO, aby wykazać zgodność realizowanych czynności przetwarzania, prowadzi następującą dokumentację dla Urzędu:

1) Rejestr czynności przetwarzania;
2) Rejestr kategorii czynności przetwarzania;
3) Ewidencję osób upoważnionych;
4) Ewidencję umów powierzenia danych osobowych Urzędu do przetwarzania;
5) Ewidencję naruszeń;
6) Analiza Ryzyka/ocena skutków dla ochrony danych
7) inną wymaganą przez RODO- dokumenty te opatrzone są pieczęcią administratora, podpisem osoby upoważnionej.

§ 21
Obowiązki kierowników referatów

1. Kierownicy referatów Urzędu, w których przetwarzane są dane osobowe zobowiązani są do stałego monitorowania zagrożeń związanych z przetwarzaniem w ramach ich komórki, a następnie do analizy ryzyka w tym obszarze.

2. W szczególności wzrost ryzyka przetwarzania danych może być związany z:
    1) wynikającej ze zmian w przepisach prawa konieczności wprowadzania nowych rozwiązań technicznych lub organizacyjnych w zakresie przetwarzania danych;
    2) stwierdzeniem naruszeń ochrony danych;
    3) wprowadzaniem modyfikacji procesu przetwarzania danych osobowych w istniejącym zbiorze;
    4) planowaniem przetwarzania danych osobowych w nowym zbiorze;
    5) planowaniem powierzenia przetwarzania danych podmiotowi zewnętrznemu;
    6) planowaniem przyjęcia powierzenia przetwarzania danych od podmiotu zewnętrznego.
3. W przypadku stwierdzenia wzrostu ryzyka, kierownik referatów w uzgodnieniu z IOD lub ASI ustala, a następnie wdraża rozwiązania minimalizujące ryzyko.

§ 22
Audyty

1. Monitorowanie przestrzegania RODO, innych przepisów o ochronie danych, polityk realizuje Administrator lub osoba przez niego wyznaczona lub Inspektor Ochrony Danych.
2. Przeprowadzenie audytu wewnętrznego w zakresie bezpieczeństwa informacji wykonuje audytor wewnętrzny lub inna wyznaczona przez ADO osoba.

§ 23
Przepisy końcowe

Polityka Ochrony Danych Osobowych wchodzi w życie z dniem jej podpisania przez Administratora.