**Załącznik nr 1**

**do zarządzenia Nr 50/2020**

**Polityka Ochrony Danych Osobowych**

**Starostwa Powiatowego w Jarocinie**

**Spis treści**

[Wprowadzenie 3](#_Toc45200187)

[Definicje 4](#_Toc45200188)

[§ 1. Obowiązek zapoznania pracowników z Polityką Bezpieczeństwa 5](#_Toc45200189)

[§ 2. Podstawy przetwarzania 5](#_Toc45200190)

[§ 3. Powierzenie przetwarzania danych osobowych 5](#_Toc45200191)

[§ 4. Udostępnienie danych osobowych 6](#_Toc45200192)

[§ 5. Realizowanie obowiązków informacyjnych 6](#_Toc45200193)

[§ 6 Prawa osoby, które dane dotyczą 7](#_Toc45200194)

[§ 7. Rejestr czynności przetwarzania danych osobowych 7](#_Toc45200195)

[§ 8. Analiza ryzyka 7](#_Toc45200196)

[§ 9. Zabezpieczenie danych osobowych 7](#_Toc45200197)

[§ 10. Zdarzenia naruszające ochronę danych osobowych 8](#_Toc45200198)

[§ 11. Postępowanie w przypadku naruszenia ochrony danych osobowych 8](#_Toc45200199)

[§ 12 Zgłaszanie naruszeń 10](#_Toc45200200)

[§ 13. Monitorowanie zabezpieczeń 10](#_Toc45200201)

[§ 14. Zasady prowadzenia ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych 11](#_Toc45200202)

[§ 15. Upoważnienie do przetwarzania danych osobowych 11](#_Toc45200203)

[§ 16. Odpowiedzialność pracownika 11](#_Toc45200204)

[§ 17. Dokumentacja przetwarzania prowadzona przez ADO 12](#_Toc45200205)

[§ 18. Obowiązki kierowników referatów 13](#_Toc45200206)

[§ 19. Audyty 13](#_Toc45200207)

[§ 20. Przepisy końcowe 14](#_Toc45200208)

# 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 Starostwo Powiatowe w Jarocinie 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 główny specjalista ds. obsługi informatycznej, zarządza systemami informatycznymi Starostwa Powiatowego w Jarocinie.

**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 Starostwie Powiatowym w Jarocinie 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. Administrator 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 Administrator 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 Administrator (powiatu jarocińskiemu) 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 Administrator;
   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 Starostwa Powiatowego w Jarocinie oraz na stronie internetowej Powiatu Jarocińskiego;
   2. wywieszeniu informacji o przetwarzaniu danych we wszystkich lokalizacjach Starostwa Powiatowego w Jarocinie 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 druku zgody na przetwarzanie jego danych osobowych;
   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, przy pomocy Inspektora Ochrony 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 Starostwie Powiatowym w Jarocinie.
3. Wniosek o wpisanie w 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 (w szczególności audytor wewnętrzny) dokonuje przeglądu analizy ryzyka regularnie, co najmniej 1 raz w roku i powiadamia Administratora o wynikach tej oceny.

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.

# § 10. 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.

# § 11. 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 niezwłocznie o tym fakcie poinformować Administratora, IOD lub ASI (w przypadku incydentów dotyczących infrastruktury IT).

3. 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.

4. 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.

5. 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.
6. W ewidencję naruszeń ochrony danych osobowych wpisuje się wszystkie naruszenia, które podlegają lub nie podlegają zgłoszeniu do organu nadzorczego.
7. 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.
8. Podobnym konsekwencjom podlegają próby karania osób uprawnionych lub pracowników za zgłoszenie naruszenia lub podejrzenia naruszenia.
9. Administrator chroni wszystkie osoby uprawnione lub pracowników zgłaszających w dobrej wierze podejrzenia zagrożenia lub naruszenia bezpieczeństwa danych, niezależnie od zasadności tych podejrzeń.

# § 12 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 spowodowało ryzyka naruszenia praw i wolności osób fizycznych lub jest to mało prawdopodobne, nie zgłasza naruszenia 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. zgłaszania naruszenie organowi nadzorczemu;
  2. powiadamia osoby, której dane dotyczą o naruszeniu;

1. Administrator Danych w przypadku stwierdzenia naruszenia podejmowanie działań mających na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.
2. Ewidencje naruszeń i związaną z tym dokumentację prowadzi Sekretarz Powiatu.

# § 13. 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:
3. okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych;
4. przestrzeganie przepisów dotyczących ochrony danych osobowych;
5. kontrolę ewidencji nośników danych;
6. kontrolę właściwej częstotliwości zmiany haseł;
7. spełnianie obowiązków informacyjnych RODO.

# § 14. Zasady prowadzenia ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych

* + 1. Administrator Danych, przy pomocy Biura Zarządu, prowadzi ewidencję wszystkich pracowników jednostki zatrudnionych przy przetwarzaniu danych osobowych i posiadających odpowiednie upoważnienia.
    2. Jakakolwiek zmiana informacji wyszczególnionej w ewidencji wymaga natychmiastowego poinformowania administratora danych.
    3. Za zgłaszanie zmian zawartych w ewidencji odpowiedzialny jest bezpośredni przełożony pracownika (Kierownik Wydziału).

# § 15. 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 operacji na danych, jak również identyfikator upoważnianej osoby w systemie informatycznym, w którym osoba ta przetwarza dane osobowe.
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.

# § 16. 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 Starostwo Powiatowe w Jarocinie 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.

# § 17. Dokumentacja przetwarzania prowadzona przez ADO

l. Integralną część polityki danych stanowią załączniki.

2. Minimalna ilość załączników obejmuje:

1. Rejestr czynności przetwarzania;
2. Rejestr kategorii czynności przetwarzania;
3. Upoważnienia do przetwarzania danych;
4. Ewidencję osób upoważnionych;
5. Ewidencję umów powierzenia danych osobowych Starostwa Powiatowego w Jarocinie do przetwarzania;
6. Rejestr umów powierzenia Starostwu Powiatowemu w Jarocinie danych osobowych do przetwarzania (kategorii czynności);
7. Ewidencję naruszeń;
8. Ogólna Analiza Ryzyka;
9. Polityka haseł;
10. Polityka czystego biurka;
11. Polityka czystego ekranu;
12. Formularz zgłoszenia i oceny incydentu;
13. Ewidencja pobrań kluczy;
14. Polityka kluczy;
15. Procedura realizacji praw osób fizycznych (z procedurą identyfikacji);
16. Zgoda na wynoszenie dokumentacji;
17. Rejestr zgód na wynoszenie dokumentacji;
18. Rejestr naruszeń;
19. Rejestr upoważnień do kluczy;
20. Inna dokumentacja wskazana przez RODO.

3. Treść załączników ustala Sekretarz Powiatu poprzez opieczętowanie dokumentu, podpisanie i opatrzenie datą.

4. Dodawanie, zmiana lub aktualizacja załączników do niniejszej polityki możliwa jest przez Sekretarza Powiatu poprzez opieczętowanie dokumentu, podpisanie i opatrzenie datą.

# § 18. Obowiązki kierowników referatów

1. Kierownicy referatów Starostwa Powiatowego w Jarocinie, 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 referatu w uzgodnieniu z IOD lub ASI ustala, a następnie wdraża rozwiązania minimalizujące ryzyko.
4. Nadzór nad kierownikami referatu, zgodnie z Regulaminem Organizacyjnym Starostwa Powiatowego w Jarocinie, prowadzą naczelnicy wydziałów.

# § 19. Audyty

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

# § 20. Przepisy końcowe

* 1. Polityka Ochrony Danych Osobowych wchodzi w życie z dniem jej podpisania przez Administratora.
  2. Zmiana polityki bezpieczeństwa wymaga zarządzenia administratora.