

REGULAMINU POWOŁANIA INSPEKTORA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY W BARDZIE.

I. Powołanie IOD

W oparciu o obowiązujące przepisy zawarte w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. zgodnie z :

- art. 37 ust. 2 lit a, Administrator Danych Osobowych podmiotu publicznego spełniając obowiązek, powołuje Inspektora Ochrony Danych Osobowych.
- art. 37 ust. 5, inspektor ochrony danych osobowych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań, o których mowa w art. 39.

1. Kwalifikacje zawodowe

- 1.1. Inspektor Ochrony Danych Osobowych powinien posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych (powinien posiadać odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych, a poziom tej wiedzy musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki; co więcej kandydat powinien też wykazać się odpowiednią wiedzą na temat danego sektora i podmiotu administratora, a także na temat operacji przetwarzania danych, ogólnej wiedzy dot. systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych).
- 1.2. W celu zweryfikowania kwalifikacji zawodowych, a w szczególności fachowej wiedzy kandydatów ubiegających się o pełnienie obowiązków Inspektora Ochrony Danych Osobowych Administrator może ustalić następujące wymagania kwalifikacyjne do wyboru:
 - a) Doświadczenie zawodowe - minimum 3 lata pełnienia obowiązków Administratora Bezpieczeństwa Informacji lub 1 rok pełnienia obowiązków Inspektora Ochrony Danych Osobowych.
 - b) Zdanie testu kompetencyjnego w celu sprawdzenia wiedzy z zakresu ochrony danych osobowych.
 - c) Posiadanie dokumentów potwierdzających ukończenie np. kursów, studiów z zakresu ochrony danych osobowych.

2. Forma zatrudnienia Inspektora Ochrony Danych Osobowych.
 - 2.1. Administrator Danych Osobowych zarządzeniem powołuje wybranego do pełnienia obowiązków Inspektora Ochrony Danych Osobowych;
 - 2.2. Inspektorem ochrony danych może zostać:
 - a) pracownik administratora lub podmiotu przetwarzającego na podstawie umowy o pracę;
 - b) osoba spoza grona pracowników - tzw. outsourcing na podstawie umowy o świadczenie usług.
3. Powołanie IOD, a ustawa z dnia 11.09.2019 r. - Prawo zamówień publicznych.
 - 3.1. W przypadku wyznaczenia IOD spoza personelu Urzędu należy uwzględnić ustawę z dnia 11.09.2019 r. - Prawo zamówień publicznych.
 - 3.2. Jeżeli wycenione zlecenie nie będzie przekraczać wartości 130 000 tys. złotych umowa nie będzie musiała być zawierana w trybie ustawy.
 - 3.3. Przy zawieraniu umowy należy uwzględnić zasady wprowadzone Zarządzeniem w/s wprowadzenia zasad rachunkowości dla Urzędu Miasta i Gminy w Bardzie.
 - 3.4. W przypadku Inspektora Ochrony Danych Osobowych, istotnym kryterium wyboru powinno być doświadczenie/kwalifikacje w zakresie ochrony danych osobowych.
4. Obowiązek zgłoszenia Inspektora Ochrony Danych Osobowych do Prezesa UODO.
 - 4.1. Na podstawie Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych Art. 10. ust. 1 Administrator Danych Osobowych w terminie 14 dni od dnia wyznaczenia Inspektora Ochrony Danych zawiadamia Prezesa Urzędu Ochrony Danych o jego wyznaczeniu.
W zawiadomieniu wskazuje imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora oraz dołącza się pełnomocnictwo udzielone w formie elektronicznej.

II. Zadania Inspektora Ochrony Danych Osobowych – art. 39 ust.1 i 2 RODO

1. Obligatoryjne zadania Inspektora Ochrony Danych Osobowych:
 - 1.1. Informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
 - a) Uzgodnienie z Administratorem procesu wykonania obowiązku informacyjnego. Opracowanie i rekomendowanie klauzul informacyjnych, zgodnie z art. 13, 14 i 15 RODO;
 - b) Uzgodnienie z Administratorem prawidłowych przesłanek legalizujących przetwarzanie danych osobowych (art. 6 i 9 Rozporządzenia 2016/679), a w przypadku stwierdzenia uchybień, pomoc w przywróceniu stanu zgodnego z prawem;
 - c) Wsparcie w zakresie zapewnienia zgodności treści umów powierzenia z wymaganiami art. 28 RODO;
 - d) Wdrożenie procesu analizowania ryzyka;

- e) Rekomendowanie rozwiązań w zakresie wprowadzania zabezpieczeń dla poszczególnych obszarów działania administratora, takich jak zabezpieczenia techniczne i równoważenie ich już na poziomie zakupowym;
 - f) Wdrożenie zasad opracowywania i aktualizowania rejestru czynności przetwarzania;
 - g) Tworzenie procedur i rozwiązań już na etapie projektowym, czyli przed przetwarzaniem danych (domyślnie je planując) oraz w trakcie przetwarzania;
 - h) Przeprowadzenie konsultacji i korzystanie z doradztwa specjalistów w zakresie spraw technicznych związanych z tworzeniem zabezpieczeń, co pozwala na przeprowadzenie wiarygodnej analizy ryzyka;
 - i) Prowadzenie szkoleń w odpowiednim zakresie dla pracowników organizacji, szczególnie w obszarach do których są upoważnieni lub wyznaczenie osoby szkolącej np. w przypadku wymaganej specjalistycznej wiedzy technicznej i realizacji tego zadania przez administratorów systemów informatycznych;
 - j) Doradzanie w obszarze zarządzania kryzysem wywołanym skargą, publikacją, wyciekem danych lub związanym z wystąpieniem incydentu bezpieczeństwa z zakresu ochrony danych osobowych, wsparcie przepływu wewnętrznej i zewnętrznej komunikacji podczas podejmowanych działań;
 - k) Wdrożenie systemu zapoznawania się przez każdego członka organizacji z obowiązującymi regulacjami z obszaru ochrony danych osobowych np. z polityką bezpieczeństwa.
- 1.2. Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- a) Przeprowadzanie audytów zgodności przetwarzania danych osobowych z Rozporządzeniem 2016/679 i innymi przepisami o ochronie danych osobowych, sporządzanie sprawozdania z audytu i przedkładanie go Administratorowi.
 - b) Przeprowadzanie, jeśli to uzasadnione, audytów bezpieczeństwa danych osobowych w Podmiotach przetwarzających, którym Zleceniodawca powierzył dane do przetwarzania.
 - c) Weryfikacja dokumentacji pod kątem zgodności z wymaganiami RODO, rekomendowanie aktualizacji dokumentacji.
- 1.3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 ocena skutków dla ochrony danych.
- Zgodnie z artykułem 35 do obowiązków Administratora, a nie IOD, należy przeprowadzanie w określonych przypadkach oceny skutków dla ochrony danych. IOD wspiera Administratora przy przeprowadzaniu takiej oceny. Zgodnie z zasadą ochrony danych w fazie projektowania, artykuł 35 nakłada na Administratora obowiązek konsultowania się z IOD przy dokonywaniu oceny skutków dla ochrony danych.

Grupa Robocza Art. 29 zaleca administratorowi konsultowanie z IOD m.in. następujących kwestii:

- a) faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych;
- b) metodologii przeprowadzenia oceny skutków dla ochrony danych;
- c) faktu, czy należy przeprowadzić wewnętrzną ocenę skutków dla ochrony danych czy też zlecić ją podmiotowi zewnętrznemu;
- d) zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- e) prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z wymogami ochrony danych (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować).

1.4. Współpraca z organem nadzorczym, np. prowadzenie korespondencji z organem nadzorczym, zarówno w trybie administracyjnym, jak i podczas kontroli aby umożliwić Urzędowi Ochrony Danych Osobowych dostęp do dokumentów i informacji w celu realizacji zadań.

1.5. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 , oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

1.6. Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących tym osobom na mocy Rozporządzenia 2016/679.

1.7. Inspektor ochrony danych wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Ten przepis wymaga od IOD aby prawidłowo ustalił priorytety w swojej pracy, ponieważ to działania mające największy wpływ na zniwelowanie największych i najbardziej dotkliwych w skutkach ryzyk.

2. Fakultatywne zadania Inspektora Ochrony Danych Osobowych:

2.1. Prowadzenie rejestru czynności przetwarzania danych.

2.2. Zadania realizowane przez administratora w ramach zasady rozliczalności np. prowadzenie rejestru umów powierzenia danych.

3. Inspektor Ochrony Danych Osobowych nie wykonuje następujących zadań:

3.1. Przekazywanie odpowiedzi na żądanie praw podmiotów danych(np. sporządzanie pisma w imieniu administratora danych).

3.2. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych.

3.3. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorcemu.

3.4. Przeprowadzenie oceny skutków dla ochrony danych.

3.5. Reprezentowanie administratora danych w ramach urzędniczych konsultacji.

III. Status Inspektora Ochrony Danych Osobowych.

1. Administrator jest obowiązany zapewnić:

1.1. Właściwe i niezwłoczne włączanie inspektora ochrony danych osobowych we wszystkie sprawy dotyczące ochrony danych osobowych - art.38 ust 1 RODO.

Inspektor ochrony danych osobowych powinien zostać poinformowany o wszystkich kwestiach dotyczących przetwarzania danych osobowych na jak wcześniejszym etapie.

1.2. Zgodnie z wytycznymi Grupy Roboczej art. 29 administrator zapewnia m.in.

1.2.1. Udział IOD w spotkaniach kadry kierowniczej, podejmowanie decyzji dotyczących przetwarzania danych osobowych;

1.2.2. Uczestnictwo IOD przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych;

- a) Administrator udziela IOD dostępu do danych osobowych oraz operacji przetwarzania, a także zapewnia wsparcie ze strony kierownictwa jednostki.
- b) Administrator zapewnia IOD odpowiednie zasoby konieczne do realizacji obowiązków w tym:
 - Odpowiedniego wsparcia finansowego, infrastrukturalnego i kadrowego;
 - Wystarczającego czasu wymaganego do realizacji zadań, m.in. zlecanie mu pracy oraz usług w odpowiednim wymiarze;
 - Komunikacji z zespołem pracowników, aby wiedzieli o jego istnieniu oraz pełnionych przez niego funkcjach;
 - Dostęp do innych referatów urzędu (np. kadry, pomoc prawna, IT);
 - Ciągłych szkoleń aktualizujących wiedzę IOD;
 - Zespołu dla IOD, jeżeli wymiar zadań nie pozwala na ich realizację samodzielnie

2. Niezależność Inspektora ochrony danych osobowych.

2.1. Administrator zapewnia by:

2.1.1. Inspektor ochrony danych osobowych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań – art.38 ust.3 RODO; Działa on niezależnie, nie są mu narzucane żadne propozycje działania dotyczące jego zakresu kompetencji. W przypadku, gdy administrator danych podejmie decyzję niezgodną z RODO oraz zaleceniami samego IOD, w takim wypadku IOD ma prawo do ustosunkowania się do tejże decyzji oraz wyrażenie własnej opinii.

2.1.2. Inspektor ochrony danych osobowych podlegał najwyższemu kierownictwu administratora.

2.1.3. Możliwość raportowania bezpośrednio do najwyższego kierownictwa.

2.1.4. Administrator nie może udzielać IOD instrukcji dotyczących sposobu rozpoznawania sprawy, środków jakie mają zostać podjęte, celu jaki powinien zostać osiągnięty, czy też faktu czy należy skontaktować się z organem nadzorczym.

2.2. Inspektor Ochrony Danych Osobowych nie może zostać odwołany ani ukarany za udzielenie określonego zalecenia, nawet jeśli jest ono niezgodne ze stanowiskiem reprezentowanym przez Administratora lub podmiot przetwarzający.

3. Konflikt interesów

3.1. Inspektor ochrony danych osobowych, może wykonywać inne prace, jednak nie może zajmować w Urzędzie stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych.

„Zgodnie z art. 38 ust. 6 RODO Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.”

3.2. Stanowiska skonfliktowane interesami z rolą Inspektora Ochrony Danych Osobowych w Urzędzie Miasta i Gminy w Bardzie:

- Burmistrz;
- Zastępca burmistrza;
- Sekretarz;
- Skarbnik;
- Informatyk;
- Kierownik USC;
- Kierownik referatu organizacyjnego;
- Kierownik referatu komunikacji społecznej;
- Kierownik referatu finansowego;
- Kierownik referatu inwestycyjnego.

3.3. Stanowisko IOD zgodnie ze strukturą organizacyjną w Urzędzie Miasta i Gminy w Bardzie podlega bezpośrednio pod najwyższe kierownictwo tj. Burmistrz Miasta i Gminy Bardo.

3.4. Przyjmuje się możliwość pełnienia funkcji IOD przez pracownika niższego szczebla, po uprzednim przeanalizowaniu obowiązków wykonywanych przez niego na zajmowanym stanowisku. Administrator zapewnia pracownikowi wymagany czasu do należytej realizacji przez niego zadań związanych z Ochroną Danych Osobowych.

3.5. Administrator odbiera od IOD oświadczenie o braku konfliktu interesów.

4. Odpowiedzialność Inspektora ochrony danych osobowych.
 - 4.1. Art. 38 ust. 3 RODO stanowi, iż IOD „nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnienie swoich zadań.
 - 4.2. Odpowiedzialność IOD zależy od charakteru umowy, na podstawie, której IOD wykonuje swoje zadania. W przypadku zatrudnienia u administratora ponosi odpowiedzialność pracowniczą. Administrator może w takim przypadku:
 - 4.2.1. Żądać naprawienia powstałej przez pracownika szkody.
 - 4.2.2. Żądać od IOD odszkodowania za wyrządzoną szkodę z tytułu niewykonania lub nienależytego wykonania obowiązków pracowniczych w wysokości wyrządzonej szkody, ale w przypadku powstania nieumyślnej szkody, nie może ono przewyższać kwoty trzymiesięcznego wynagrodzenia przysługującego pracownikowi w dniu wyrządzenia szkody.
 - 4.2.3. Rozwiązać stosunek pracy.
 - 4.3. Odpowiedzialność IOD za wykonywanie obowiązków w przypadku zatrudnienia IOD na podstawie umowy cywilnoprawnej.
 - 4.3.1. Odpowiedzialność cywilna:

W przypadku, gdy IOD współpracuje z ADO na podstawie umowy o świadczeniu usług, do której zgodnie z art. 750 Ustawy z dnia 23.04.1964 roku – Kodeks Cywilny stosuje się przepisy o zleceniu, kwestię odpowiedzialności IOD w stosunku do ADO należy w pierwszej kolejności rozpatrywać na zasadach określonych w art. 471 Kodeksu Cywilnego (tzw. odpowiedzialność kontraktowa).

Powyższe oznacza, że IOD ponosi odpowiedzialność za szkodę wyrządzoną ADO, gdy spełnione będą ogólne przesłanki tej odpowiedzialności, tj.:

 - a) wystąpi zdarzenie powodujące szkodę;
 - b) wystąpi szkoda;
 - c) wystąpi adekwatny związek przyczynowy między zdarzeniem a szkodą (czyli gdy szkoda będzie bezpośrednim następstwem zdarzenia).
 - 4.3.2. Odpowiedzialność karna:

IOD może ponosić odpowiedzialność karną na podstawie art. 107 i 108 ustawy o ochronie danych osobowych, gdyż są to przestępstwa powszechne, tzn. mogą być popełnione przez każdego, po zaistnieniu znamion tych przestępstw:

 - a) Art. 107. Nielegalne przetwarzanie danych osobowych.
 - Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
 - Jeżeli czyn w/w dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

b) Art. 108. Udaremnianie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych, niedostarczenie Prezesowi UODO danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej.

- Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
- Tej samej karze podlega kto, w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, nie dostarcza danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarcza dane, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej.

4.3.3. Odpowiedzialność administracyjna:

IOD nie podnosi odpowiedzialności administracyjnej w związku z pełnieniem swojej funkcji. Zgodnie z art. 101 ustawy o ochronie danych osobowych, Prezes Urzędu może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż:

- a) jednostka sektora finansów publicznych,
- b) instytut badawczy,
- c) Narodowy Bank Polski.

w drodze decyzji, administracyjną karę pieniężną na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

Takim podmiotem, o którym mowa w art. 101 ustawy, jest ADO, a także podmiot przetwarzający.

IV. Zastępstwo Inspektora Ochrony Danych Osobowych.

1. Powołanie zastępcy IOD

- 1.1. Administrator może wyznaczyć zastępcę inspektora ochrony danych osobowych zgodnie z art. 11a ust. 1 ustawy o ochronie danych osobowych.
- 1.2. Nie ma obowiązku powoływania zastępcy IOD jak jest to w przypadku powołania samego IOD. Administrator sam powinien ocenić czy jest konieczność i sens powołania zastępcy i poniesienia w związku z tym dodatkowych kosztów.
- 1.3. Zastępca inspektora ochrony danych wykonuje takie same obowiązki jak sam inspektor, które zostały wymienione w dziale: II. Zadania Inspektora Ochrony Danych Osobowych – art. 39 ust.1 i 2 RODO.
- 1.4. Zastępca IOD, jako że może wykonywać takie same obowiązki jak inspektor – powinien spełniać również tożsame wymogi określone w dziale - I. Powołanie IOD.
- 1.5. Dodatkowo Administrator powinien brać pod uwagę także następujące kryteria
 - 1.5.1. Rodzaj prowadzonej działalności,
 - 1.5.2. Rozmiar organizacji,
 - 1.5.3. Charakter czynności przetwarzania,

- 1.5.4. Strukturę organizacyjną,
- 1.5.5. Prawdopodobieństwo powstania zagrożenia dla ochrony danych osobowych w sytuacji czasowej nieobecności IOD,
- 1.5.6. Zapewnienie ciągłości działania organizacji,
- 1.5.7. Rzeczywisty i przewidywany poziom dyspozycyjności IOD (który może być mniejszy w zależności od formy współpracy, a także od tego, czy inspektor obsługuje również innych administratorów),
- 1.5.8. Potrzeba zapewnienia wsparcia kadrowego dla IOD,
- 1.5.9. Zgodnie z Wytycznymi Grupy Roboczej art.29, administrator bierze pod uwagę stopień skomplikowania procesów przetwarzania danych w celu zapewnienia odpowiednich środków organizacyjnych i technicznych aby realizować skuteczną i efektywną ochronę danych osobowych - takim rozwiązaniem może być wyznaczenie zastępcy IOD,
- 1.5.10. Wyznaczając zastępcę IOD administrator bierze pod uwagę także jego usytuowanie w strukturze organizacyjnej. Zastępca IOD powinien bezpośrednio podlegać najwyższemu kierownictwu administratora z uwagi na zapewnienie mu niezależności przy wykonywaniu zadań,
- 1.5.11. Zadania zastępcy inspektora należy określić w taki sposób, by rozgranaczyć okresy obecności i nieobecności inspektora. Pozwala to na zapewnienie przejrzystości prawnej, usprawnienie organizacji oraz zapobiega konfliktom interesów członków zespołu realizującego zadania z zakresu ochrony danych osobowych (jak wskazano w Wytycznych Grupy Roboczej Art. 29) Nic także nie stoi na przeszkodzie wprowadzeniu rozwiązania, zgodnie z którym zastępca inspektora ochrony danych będzie wykonywał swoje zadania wyłącznie w razie nieobecności IOD.

BURMISTRZ
Miasta i Gminy Bardo
mgr inż. Krzysztof Żegański



