## ZARZĄDZENIE NR

# **PREZYDENTA MIASTA POZNANIA**

**z dnia 18 sierpnia 2025 r.**

|  |  |
| --- | --- |
| w sprawie | **określenia zasad współpracy Urzędu Miasta Poznania z miejskimi jednostkami organizacyjnymi w zakresie wspólnego systemu ochrony danych osobowych** |

Na podstawie art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 1465 ze zm.) oraz art. 37-39 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) – Dz. Urz. UE. L Nr 119, str. 1, z 2018 r. Nr 127, poz. 2 oraz z 2021 r. Nr 74, poz. 35 zarządza się, co następuje:

**§ 1**

Ilekroć w zarządzeniu jest mowa o:

1) RODO – należy przez to rozumieć rozporządzenie 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) – Dz. Urz. UE. L Nr 119, str. 1, z 2018 r. Nr 127, poz. 2 oraz z 2021 r. Nr 74, poz. 35;

2) ustawie – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);

3) KRI – należy przez to rozumieć rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773);

4) Urzędzie – należy przez to rozumieć Urząd Miasta Poznania;

5) Mieście – należy przez to rozumieć Miasto Poznań jako jednostkę samorządu terytorialnego;

6) m.j.o. – należy przez to rozumieć miejską jednostkę organizacyjną;

7) Administratorze Danych Osobowych – należy przez to rozumieć m.j.o., która przystąpiła do współpracy z Urzędem w zakresie zarządzania bezpieczeństwem informacji i ochrony danych osobowych, w imieniu której działa jej kierownik.

**§ 2**

1. W związku z wolą zapewnienia w Mieście jednolitych standardów zarządzania bezpieczeństwem informacji i ochrony danych osobowych umożliwia się podjęcie współpracy pomiędzy m.j.o. a Urzędem. Wykaz m.j.o., które wyraziły chęć przystąpienia do współpracy, zawiera załącznik nr 1 do zarządzenia.

2. Współpraca jest realizowana za pośrednictwem Inspektora Ochrony Danych w Biurze Cyfryzacji i Cyberbezpieczeństwa Urzędu oraz jego zespołu, składającego się z pracowników Urzędu o odpowiednich kwalifikacjach zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz o umiejętnościach niezbędnych do wypełniania zadań, o których mowa w art. 39 RODO.

3. W celu rozpoczęcia współpracy zainteresowana m.j.o. zawrze z Urzędem porozumienie, na mocy którego zostaną wyznaczone osoby do pełnienia funkcji Inspektora Ochrony Danych oraz funkcji Zastępcy Inspektora Ochrony Danych dla tej m.j.o. Wzór porozumienia określa załącznik nr 2 do zarządzenia.

4. Wyznaczony Inspektor Ochrony Danych w wykonywaniu swej funkcji jest niezależny i merytorycznie podlega wyłącznie najwyższemu kierownictwu Administratora Danych Osobowych, a organizacyjnie zastępcy dyrektora ds. Cyberbezpieczeństwa Biura Cyfryzacji i Cyberbezpieczeństwa Urzędu.

**§ 3**

1. Zakres zadań Inspektora Ochrony Danych określają przepisy o ochronie danych osobowych.

2. Do podstawowych obowiązków Inspektora Ochrony Danych wykonującego tę funkcję dla Administratora Danych Osobowych w ramach współpracy należy:

1) monitorowanie przestrzegania RODO oraz polityk Administratora Danych Osobowych lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych;

2) informowanie Administratora Danych Osobowych i podmiotu przetwarzającego oraz ich pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradzanie im w sprawach z tym związanych, w tym organizowanie szkoleń z zakresu ochrony danych;

3) przygotowywanie planu sprawdzeń i przeprowadzanie planowych oraz doraźnych weryfikacji zgodności sposobu przetwarzania danych osobowych z obowiązującym prawem i sporządzanie w tym zakresie sprawozdań dla Administratora Danych Osobowych;

4) zapobieganie naruszeniom ochrony danych osobowych, a w przypadku ich stwierdzenia podejmowanie działań poprzez udzielanie wsparcia i konsultacji kierownikowi m.j.o. w zakresie:

a) wskazywania zaleceń zmierzających do przywrócenia stanu zgodnego z prawem,

b) zawieranych umów lub innych instrumentów prawnych regulujących przetwarzanie danych osobowych przez podmiot przetwarzający,

c) koordynowania prowadzenia dokumentacji stwierdzającej naruszenia bezpieczeństwa danych osobowych,

d) koordynowania prowadzenia innej dokumentacji wymaganej przez RODO, w szczególności wskazanej w § 4 pkt 4;

5) udzielanie na żądanie Administratora Danych Osobowych zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

6) współpraca z Prezesem Urzędu Ochrony Danych Osobowych;

7) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

8) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO;

9) bieżące wsparcie Administratora Danych Osobowych w zakresie ochrony danych osobowych, w szczególności stosowania przepisów RODO, ustawy oraz innych przepisów dotyczących przetwarzania danych osobowych, obejmujące w szczególności opiniowanie regulacji wewnętrznych, formularzy, umów i czynności przetwarzania realizowanych przez Administratora Danych Osobowych pod względem zgodności z przepisami o ochronie danych osobowych.

**§ 4**

Do zadań Administratora Danych Osobowych należy w szczególności:

1) zawiadamianie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu Inspektora Ochrony Danych, zgodnie z art. 10 ustawy;

2) wyznaczenie w strukturze organizacyjnej Koordynatora Ochrony Danych Osobowych, który będzie współpracował z wyznaczonym Inspektorem Ochrony Danych;

3) udostępnienie zgodnie z art. 11 i art. 11a ust. 3 ustawy danych wyznaczonego Inspektora Ochrony Danych oraz Zastępcy Inspektora Ochrony Danych, w zakresie: imienia, nazwiska, adresu mailowego, a w przypadku zmiany osób wykonujących te funkcje, aktualizacja tych danych;

4) prowadzenie i aktualizowanie podstawowej dokumentacji z zakresu przetwarzania danych osobowych, wymaganej przez RODO:

a) rejestru czynności przetwarzania danych osobowych – na podstawie art. 30 ust. 1 RODO,

b) rejestru kategorii czynności przetwarzania danych osobowych – na podstawie art. 30 ust. 2 RODO,

c) rejestru incydentów – na podstawie art. 33 ust. 5 RODO,

d) oceny skutków dla ochrony danych osobowych (DPIA) – na podstawie art. 35 RODO;

5) korzystanie ze wskazanych przez Biuro Cyfryzacji i Cyberbezpieczeństwa Urzędu narzędzi do wymiany informacji i przesyłania dokumentów pomiędzy Administratorem Danych Osobowych a wyznaczonym Inspektorem Ochrony Danych;

6) korzystanie ze wskazanego przez Biuro Cyfryzacji i Cyberbezpieczeństwa Urzędu oprogramowania do prowadzenia rejestrów, o których mowa w § 4 pkt 4 lit. a, b i c oraz innych czynności wymaganych przez RODO;

7) zapewnienie, by wyznaczony Inspektor Ochrony Danych był niezwłocznie informowany o wszystkich sprawach dotyczących ochrony danych osobowych realizowanych u Administratora Danych Osobowych, w tym aby uzyskiwał dostęp do danych osobowych i czynności przetwarzania, w szczególności poprzez przekazywanie w wersji elektronicznej projektów umów oraz innych dokumentów, w zakresie których dochodzi do przetwarzania danych osobowych lub powierzenia przetwarzania danych osobowych, w celu zaopiniowania ich pod względem zgodności z przepisami o ochronie danych osobowych;

8) zapewnienie warunków wyznaczonemu Inspektorowi Ochrony Danych do sprawnego przeprowadzania sprawdzeń w zakresie wypełniania wymogów i wytycznych bezpieczeństwa informacji i ochrony danych osobowych u Administratora Danych Osobowych;

9) podejmowanie decyzji o realizacji zaleceń wystosowanych przez wyznaczonego Inspektora Ochrony Danych.

**§ 5**

W miarę możliwości, w ramach realizacji działań, o których mowa w § 19 ust. 2 pkt 14 KRI, dbając o jednolitość w zakresie wdrażania systemowego zarządzania bezpieczeństwem informacji oraz zastosowania odpowiednich środków technicznych i organizacyjnych określonych w art. 32 ust. 1 RODO, Biuro Cyfryzacji i Cyberbezpieczeństwa Urzędu (w porozumieniu z właściwym dla danej m.j.o. wydziałem nadzorującym Urzędu) zapewnia przeprowadzenie audytów w zakresie bezpieczeństwa informacji w m.j.o., które przystąpiły do współpracy na zasadach określonych w zarządzeniu, i wyłania wykonawcę audytów.

**§ 6**

Wykonanie zarządzenia powierza się kierownikom m.j.o., które przystąpią do współpracy na zasadach określonych w zarządzeniu oraz dyrektorowi Biura Cyfryzacji i Cyberbezpieczeństwa Urzędu.

**§ 7**

Traci moc zarządzenie Nr 512/2019/P Prezydenta Miasta Poznania z 17 czerwca 2019 r. w sprawie określenia zasad współpracy Urzędu Miasta Poznania z miejskimi jednostkami organizacyjnymi w zakresie wspólnego systemu ochrony danych osobowych ze zmianami.

**§ 8**

Zarządzenie wchodzi w życie z dniem podpisania.

PREZYDENT MIASTA POZNANIA

(-) Jacek Jaśkowiak