

ZARZĄDZENIE NR 149/2019
BURMISTRZA CIECHOCINKA
z dnia 10 października 2019 roku

w sprawie organizacji systemu ochrony danych osobowych
w Urzędzie Miejskim w Ciechocinku

Na podstawie art. 24 i 37 ust. 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) – dalej, jako „RODO” oraz art. 9 ust. 1 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (*Dz. U. z 2018 r., poz. 1000*) - **zarządza się co następuje:**

§ 1. Przetwarzanie danych osobowych w Urzędzie Miejskim w Ciechocinku służy realizacji obowiązków oraz uprawnień określonych przepisami prawa, w szczególności realizacji zadań własnych gminy wynikających z ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (*T. jedn.: Dz. U. z 2019 r., poz. 506*) i zadań zleconych z zakresu administracji państwowej.

§ 2.

1. **Administratorem Danych** osobowych w Gminie Miejskiej Ciechocinek jest Burmistrz Ciechocinka.
2. Obowiązki wynikające z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) – dalej, jako „RODO” oraz ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (*Dz. U. z 2018 r., poz. 1000*) Burmistrz powierza:
 - 1) w zakresie ogólnego nadzoru nad przestrzeganiem zasad ochrony danych osobowych w Urzędzie – **Inspektorowi Ochrony Danych;**
 - 2) w zakresie zarządzania i bieżącego nadzoru nad przestrzeganiem zasad ochrony danych osobowych w systemach informatycznych Urzędu – **Administratorowi Systemów Informatycznych;**
 - 3) w zakresie realizacji ustalonych procedur bezpieczeństwa przetwarzania danych osobowych w podległych komórkach organizacyjnych – **Administratorom Grup Informacji;**

- a) Sekretarzowi Miasta – w grupie: Biuro Organizacyjne, Referat Społeczno-Administracyjny, Biuro Organów Samorządowych, Kadry,
- b) Kierownikowi Referatu Finansowego – w grupie Referat Finansowy,
- c) Kierownikowi Referatu Gospodarki Terenami i Ochrony Środowiska – w grupie Referat Gospodarki Terenami i Ochrony Środowiska,
- d) Kierownikowi Referatu Gospodarki Miejskiej - w grupie Referat Gospodarki Miejskiej, Monitoring Miejski,
- e) Kierownikowi Kultury, Sportu i Promocji Miasta – w grupie Kultura, Sport i Promocja Miasta;
- f) Pełnomocnikowi ds. ochrony informacji niejawnych i OC – w grupie sprawy wojskowe, sprawy obronne, obrona cywilna, zarządzanie kryzysowe,
- g) Inspektorowi ds. oświaty – w grupie Oświata.

§ 3.

1. Na stanowisko **Inspektora Ochrony Danych** został powołany z dniem 18 lipca 2018 roku Pełnomocnik ds. ochrony informacji niejawnych i OC – **Mirosław Ciuryło**.
2. Na stanowisko **Administratora Systemów informatycznych** został wyznaczony z dniem 1 stycznia 2019 roku informatyk Urzędu.

§ 4.

1. **Inspektor Ochrony Danych** wykonuje zadania z zakresu ochrony danych osobowych przy pomocy Administratora Systemów Informatycznych oraz Administratorów Grup informacji.
2. **Inspektor Ochrony Danych** realizuje następujące zadania:
 - 1) informuje Administratora Danych, Administratora Systemów Informatycznych i pracowników przetwarzających dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradza im w tej sprawie;
 - 2) sprawuje stałą kontrolę i sprawdza zgodność procesów przetwarzania danych osobowych z przepisami regulującymi zasady ochrony danych osobowych;
 - 3) monitoruje przestrzeganie rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Administratora Danych, w tym monitoruje podział obowiązków, podejmuje działania zwiększające świadomość personelu uczestniczącego w operacjach przetwarzania oraz prowadzi wewnętrzne audyty;

- 4) organizuje i realizuje szkolenie personelu uczestniczącego w operacjach przetwarzania danych osobowych;
- 5) udziela na żądanie Administratora Danych zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej realizację;
- 6) współpracuje z organem nadzorczym;
- 7) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach;
- 8) pełni funkcję punktu kontaktowego dla osób, których dane przetwarzane są w Urzędzie;
- 9) prowadzi rejestr czynności przetwarzania danych osobowych;
- 10) prowadzi rejestru kategorii czynności przetwarzania danych osobowych w imieniu Administratora Danych;
- 11) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;
- 12) prowadzi rejestr naruszeń ochrony danych osobowych.

§ 5.

1. **Sekretarza Miasta** zobowiązuje się, w terminie 60 dni od dnia wejścia w życie niniejszego zarządzenia, do uzupełnienia akt osobowych pracowników Urzędu Miejskiego zatrudnionych przy przetwarzaniu danych osobowych o:
 - 1) upoważnienia do przetwarzania danych osobowych, wydane przez Administratora Danych;
 - 2) zgodę na przetwarzanie danych osobowych;
 - 3) klauzulę (w zakresie obowiązków) dotyczącą indywidualnej odpowiedzialności dyscyplinarnej i karnej za przestrzeganie przepisów o ochronie danych osobowych;
 - 4) zobowiązanie do zachowania w tajemnicy zasad bezpieczeństwa danych osobowych stosowanych w Urzędzie w czasie ich przetwarzania , nawet po ustaniu stosunku pracy;
 - 5) oświadczenie o zapoznaniu się z aktualnymi przepisami dotyczącymi ochrony danych osobowych.
2. Udostępnianie danych osobowych pracowników Urzędu i osób ujętych w ewidencji ludności do celów innych, niż określonych w § 1 niniejszego zarządzenia, odbywa się wyłącznie za pośrednictwem **Sekretarza Miasta**.

§ 6.

1. **Administrator Systemów Informatycznych** wykonuje zadania z zakresu ochrony danych osobowych, przetwarzanych w systemach informatycznych Urzędu, we współpracy z Inspektorem Ochrony Danych, któremu podlega pod względem merytorycznym.
2. **Administrators Systemów Informatycznych** zobowiązuje się do prowadzenia:
 - 1) ewidencji identyfikatorów i pierwszych haseł dostępu użytkowników systemów informatycznych przetwarzających dane osobowe;
 - 2) ewidencji napraw, konserwacji i likwidacji urządzeń informatycznych, w których przetwarzane są dane osobowe;
 - 3) ewidencji kopii zapasowych baz danych w których przetwarzane są dane osobowe;
 - 4) ewidencji sprzętu informatycznego, służącego do przetwarzania danych osobowych;
 - 5) ewidencji oprogramowania zainstalowanego w systemach informatycznych przetwarzających dane osobowe;
 - 6) ewidencji kontroli klasyfikowanych nośników informacji;
 - 7) dziennika działania Administratora Systemów Informatycznych.

§ 7.

Administratorów Grup Informacji zobowiązuje się do przestrzegania przepisów z zakresu ochrony danych osobowych, wymienionych w § 1 niniejszego zarządzenia, w szczególności poprzez:

- 1) określanie indywidualnych zakresów obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych;
- 2) zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie;
- 3) występowanie z wnioskiem do Administratora Danych, poprzez Inspektora Ochrony Danych, o upoważnienie podległego pracownika do przetwarzania danych osobowych;
- 4) wykonywanie zaleceń Inspektora Ochrony Danych w zakresie ochrony danych osobowych;
- 5) opracowywanie i prowadzenie imiennych kart uprawnień do działań na zbiorach danych osób zatrudnionych przy przetwarzaniu danych osobowych oraz przekazywanie ich Inspektorowi Ochrony Danych;

- 6) przekazywanie na bieżąco Inspektorowi Ochrony Danych aktualnych danych z zakresu:
 - a) wykazu baz danych, w których przetwarzane są dane osobowe;
 - b) lokalizacji budynków i pomieszczeń, w których są przetwarzane dane osobowe;
- 7) stwarzanie warunków organizacyjnych i technicznych, umożliwiających spełnienie wymogów przepisów o ochronie danych osobowych;
- 8) udostępnianie danych osobowych ze zbiorów danych odbiorcom zgodnie z obowiązującymi procedurami i prowadzenie ewidencji udostępnień;
- 9) prowadzenie bieżących kontroli stanu ochrony danych osobowych.

§ 8. 1. Z dniem 1 listopada 2019 roku wprowadza się w Urzędzie Miejskim w Ciechocinku do powszechnego stosowania:

- 1) Politykę ochrony danych osobowych Urzędu Miejskiego w Ciechocinku – wersja 1.0;
 - 2) Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych Urzędu miejskiego w Ciechocinku – wersja 1.0;
 - 3) Procedury bezpieczeństwa przetwarzania danych osobowych – wersja 1.0.
- 2. Inspektor Ochrony Danych do dnia 31 grudnia 2019 roku - sporządzi i przekaże Administratorom Grup Informacji wyciągi z dokumentów wymienionych w ust. 1 pkt 1- 3.**
- 3. Administrator Systemów Informatycznych do 31 grudnia 2019 roku:**
- 1) nada wszystkim osobom zatrudnionym na stanowiskach związanych z dostępem do danych osobowych pierwsze hasła dostępu oraz założy im konta w systemach teleinformatycznych;
 - 2) sprawdzi i dostosuje ustawienia zabezpieczeń systemów informatycznych do wymogów *Polityki ochrony danych osobowych*;
 - 3) opracuje i przedstawi Burmistrzowi do dnia 31 grudnia 2019 roku wykaz potrzeb sprzętowych i oprogramowania informatycznego.
- 4. Dokumenty: *Polityka ochrony danych osobowych* i *Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych* są dokumentami stanowiącymi **Tajemnicę przedsiębiorcy** i udostępniane są osobom zatrudnionym w Urzędzie w zakresie niezbędnym do wykonywanych obowiązków służbowych przez Inspektora Ochrony Danych.**

§ 9. Zobowiązuje się Kierowników Referatów – Administratorów Grup Informacji do przekazania Inspektorowi Ochrony Danych, w terminie 30

dni od dnia wejścia w życie niniejszego zarządzenia, kart uprawnień pracowników zatrudnionych przy przetwarzaniu danych osobowych.

§10. Osoby nie przestrzegające przepisów w zakresie ochrony danych osobowych podlegają sankcjom przewidzianym w art. 107 i 108 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).

§ 11. Tracą moc:

- 1) zarządzenie nr 166/11 z dnia 27 grudnia 2011 roku w sprawie ochrony danych osobowych;
- 2) zarządzenie nr 167/11 z dnia 27 grudnia 2011 roku w sprawie wdrożenia systemu bezpieczeństwa informacji.

§ 12. Zarządzenie wchodzi w życie z dniem podpisania.

Do wiadomości:

1. Małgorzata SZWAJKOWSKA
2. Agnieszka LEWANDOWSKA
3. Barbara CICHOWSKA
4. Magdalena ZWIERZCHOWSKA-DROŹDŹA
5. Andrzej SZCZEPANOWSKI
6. Janusz HAWIK
7. Inspektor ds. oświaty
8. Mirosław CIURYŁO