

ZARZĄDZENIE NR 219/2020
BURMISTRZA MIASTA KAMIENNA GÓRA

z dnia 24 lipca 2020 r.

w sprawie: wprowadzenia procedury sprawdzeń zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi procedurami wdrożonymi w Urzędzie Miasta Kamienna Góra

Na podstawie § 16 Polityki Bezpieczeństwa Przetwarzania Danych w Urzędzie Miasta Kamienna Góra wprowadzonej Zarządzeniem Nr 112/2019 Burmistrza Miasta Kamienna Góra z dnia 19 marca 2019 r. oraz 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. U. UE. L.2016 poz. 119), zarządzam co następuje:

§ 1. Wprowadzam procedurę sprawdzeń zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi procedurami wdrożonymi w Urzędzie Miasta Kamienna Góra, która stanowi załącznik Nr 1 do niniejszego zarządzenia .

§ 2. Traci moc zarządzenie nr 51/2020 Burmistrza Miasta Kamienna Góra z dnia 20 lutego 2020 r. w sprawie wprowadzenia procedury sprawdzeń zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi procedurami w Urzędzie Miasta Kamienna Góra.

§ 3. Wykonanie zarządzenia powierzam Inspektorowi ochrony danych.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ
MIASTA KAMIENNA GÓRA

Janusz Chodurawicz
Janusz Chodurawicz

Procedura sprawdzeń zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi procedurami wdrożonymi w Urzędzie Miasta Kamienna Góra

§ 1. 1. Procedura określa zasady sprawdzenia zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi procedurami wdrożonymi w Urzędzie Miasta Kamienna Góra, zwanym dalej Urząd.

§ 2. 2. Przedmiotem sprawdzeń jest przestrzeganie przepisów prawa oraz zasad i obowiązków określonych w dokumentacji przetwarzania danych wdrożonej w Urzędzie Miasta Kamienna Góra przez komórki organizacyjne Urzędu.

§ 3. 3. Zakres sprawdzeń obejmuje:

1. przestrzeganie zapisów zawartych w Polityce Bezpieczeństwa Przetwarzania Danych;
2. przestrzeganie zapisów zawartych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych;
3. przestrzeganie zapisów zawartych w Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych;
4. przestrzeganie zapisów zawartych w Zarządzeniu Nr 8/2012 Burmistrza Kamiennej Góry z dnia 30 stycznia 2012 r. w sprawie używania legalnego oprogramowania na stanowiskach pracy w Urzędzie Miasta w Kamiennej Górze;
5. przestrzeganie zapisów zawartych w Zarządzeniu Nr 136/2018 Burmistrza Miasta Kamienna Góra z dnia 25 kwietnia 2018 r. w sprawie wprowadzenia procedury zabezpieczania pomieszczeń Urzędu Miasta Kamienna Góra;
6. zgodność z prawem przetwarzanie danych osobowych;
7. zasady przetwarzania danych osobowych - zgodnie z art. 5 ust. 1 Rozporządzenia;
8. nadawanie upoważnienia do przetwarzania danych osobowych;
9. ewidencję osób upoważnionych do przetwarzania danych osobowych;
10. procedurę nadawania uprawnień do pracy w systemie informatycznym;
11. rejestr czynności przetwarzania;
12. poprawność powierzenia danych - umowy powierzenia przetwarzania danych osobowych;
13. poprawność przekazywania danych osobowych do państw trzecich i instytucji międzynarodowych;
14. poprawność zapisów dotyczących przetwarzania danych w umowach i regulaminach;
15. zabezpieczenie fizyczne danych osobowych w formie papierowej;
16. zabezpieczenie fizyczne danych osobowych w formie elektronicznej;
17. zabezpieczenie systemowe danych osobowych w formie elektronicznej;
18. procedury i zasady postępowania realizowane przez osoby upoważnione;
19. procedury oraz tworzenie kopii zapasowych;
20. procedury wysyłania sprzętu do serwisu, na którym są przetwarzane dane osobowe;
21. procedury oraz udostępnianie danych osobowych;
22. procedury oraz niszczenie dokumentów zawierających dane osobowe (papierowe oraz elektroniczne nośniki danych);
23. procedury oraz zabezpieczenie danych po opuszczeniu stanowiska pracy;
24. sprawdzenia obowiązku informacyjnego wobec osoby fizycznej;

25. sprawdzenie podstawy prawnej przetwarzania danych;
26. szkolenia z zakresu ochrony danych osobowych;
27. szkolenia z zakresu bezpiecznej pracy w systemie informatycznym służącym do przetwarzania danych osobowych;
28. oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa Przetwarzania Danych;
29. ustawienie sprzętu komputerowego na stanowisku pracy - czy uniemożliwia dostęp do ekranów monitorów osobom nieupoważnionym.

§ 4. Sposób przeprowadzenia sprawdzenia:

1. przeprowadzenie oględzin pomieszczenia;
2. zebranie ustnych informacji od osób, które są objęte sprawdzeniem;
3. zebranie pisemnych wyjaśnień od osób, które są objęte sprawdzeniem;
4. sprawdzenie zabezpieczeń systemów informatycznych poprzez wykonanie koniecznych czynności przez osoby upoważnione, w szczególności do zarządzania systemami informatycznymi.

§ 5. Sposób dokumentowania sprawdzenia może obejmować:

1. utrwalenie danych z systemu informatycznego w postaci wydruku;
2. sporządzenia notatki z czynności, zebranych wyjaśnień i przeprowadzonych oględzin;
3. sporządzenie kopii z otrzymanych dokumentów;
4. sporządzanie kopii z zapisów rejestrów systemów informatycznych lub konfiguracji technicznych środków zabezpieczeń;
5. odebranie wyjaśnień od osoby, której czynności objęto sprawdzeniem.

§ 6.

1. Inspektor ochrony danych, zgodnie z § 16 ust. 6 Polityki Bezpieczeństwa Przetwarzania Danych, po zebraniu materiału pozwalającego ocenić zgodność przetwarzania danych osobowych przez osoby upoważnione, sporządza sprawozdanie.

2. Sprawozdanie zawiera elementy zgodne z zapisami § 16 ust. 6 Polityki Bezpieczeństwa Przetwarzania Danych.

3. Sprawozdanie zostaje przekazane kierownikowi komórki organizacyjnej celem zapoznania się z wnioskami wynikającymi ze sprawozdania.

4. Kierownik komórki organizacyjnej w ciągu 7 dni od daty przekazania sprawozdania powinien zapoznać się z jego treścią i podpisać sprawozdanie bez uwag lub złożyć pisemne uwagi do sprawozdania w ww. terminie lub odmówić podpisania sprawozdania.

5. Odmowa podpisania sprawozdania przez kierownika komórki organizacyjnej nie stanowi przeszkody do podejmowania dalszych czynności wynikających ze sprawozdania.

6. Inspektor ochrony danych nie później niż 30 dni od zakończenia sprawdzenia przekazuje sprawozdanie z planowanego sprawdzenia Administratorowi Danych.

§ 7. Inspektor ochrony danych, zgodnie z § 17 Polityki Bezpieczeństwa Przetwarzania Danych, poza sprawdzeniami planowanymi może dokonać sprawdzeń doraźnych.

§ 8. Inspektor ochrony danych sporządza plan sprawdzeń zgodności przetwarzania danych do 31 stycznia i przedstawia go do zatwierdzenia Administratorowi danych.

§ 9. Plan sprawdzeń za rok 2020 Inspektor ochrony danych przedstawi Administratorowi danych do 31 sierpnia 2020 r.

§ 10. Plan sprawdzeń musi zawierać:

1. nazwę komórki organizacyjnej wraz z nr pokoju;
2. planowany termin sprawdzenia;

3. zakres sprawdzenia, tj. co podlega kontroli, np.: system informatyczny, zabezpieczenie pomieszczeń, udostępnienie danych.

§ 11. Kierownik komórki organizacyjnej co najmniej na 7 dni przed planowaną kontrolą musi zostać poinformowany o planowanym sprawdzeniu.