

INSTRUKCJA W SPRAWIE TRYBU POSTĘPOWANIA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

§ 1

I. Przepisy ogólne.

1. Urząd jest uprawniony do uzyskiwania i przetwarzania danych osobowych w celu realizacji zadań określonych w ustawie.
2. Celem wykonania zadań wymienionych w ust. 1 urząd ma prawo do zbierania danych osobowych bez zgody zainteresowanego:
 - a) imię i nazwisko,
 - b) imiona rodziców,
 - c) data i miejsce urodzenia,
 - d) adres zamieszkania lub pobytu,
 - e) numer PESEL i NIP,
 - f) płeć,
 - g) zawód,
 - h) wykształcenie,
 - i) seria i numer dowodu osobistego lub paszportu,
 - j) stan cywilny i rodzinny,
 - k) status majątkowy,
 - l) okres i miejsce zatrudnienia oraz inne okresy zdarzeń stanowiących podstawę określenia sytuacji prawnej,
 - m) imiona i nazwiska oraz PESEL dzieci i małżonków.

Jednakże czynności związane z gromadzeniem, przetwarzaniem i przechowywaniem tych informacji muszą być wykonywane z zachowaniem wszystkich wymogów nałożonych ustawą i rozporządzeniem.

3. Informacja podlegająca ochronie jest przechowywana i przetwarzana w zbiorach w postaci tradycyjnej (akta, rejestry itp.) oraz w postaci elektronicznej (sieć informatyczna, systemy informatyczne, oprogramowanie itp.).
4. Administrator Bezpieczeństwa Informacji wyznaczony przez Administratora Danych Osobowych jest odpowiedzialny za bezpieczeństwo danych osobowych w zbiorach danych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń i systemów, w których przetwarzane są dane osobowe oraz za podejmowanie działań w przypadku naruszeń zabezpieczeń.
5. Pracownicy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani do ścisłego przestrzegania wszystkich przepisów prawa oraz wewnętrznych zarządzeń i instrukcji regulujących przetwarzanie danych osobowych.
6. Pracownicy odpowiedzialni za zabezpieczenie zbiorów danych są zobowiązani dołożyć wszelkich starań, aby przechowywane w zbiorach danych dane podlegające ochronie nie dostały się w posiadanie osób i instytucji do tego nieupoważnionych.



II. Zbiory danych w postaci tradycyjnej.

1. Akta zawierające dane osobowe podlegają ochronie.
2. Akta zawierające dane osobowe zbierane są w teczkach uporządkowanych według kolejności zdarzeń.
3. Akta powinny zawierać całą historię zmian informacji dotyczących danych osobowych, łącznie z dokumentami, które są nieaktualne, ale stanowiły podstawę do wydania decyzji administracyjnej lub podjęcia innych działań nałożonych na urząd przepisami prawnymi.
4. Akta muszą być przechowywane w miejscach niedostępnych dla osób nieupoważnionych, w pomieszczeniach i w szafach zamykanych na klucz.
5. Dostęp do akt zawierających dane osobowe mogą mieć tylko osoby upoważnione przez Administratora Danych Osobowych.
6. Administrator Bezpieczeństwa Informacji prowadzi *Rejestr upoważnień do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach* zawierający informacje o upoważnionych pracownikach oraz okresie ważności upoważnienia do przetwarzania danych osobowych. Upoważnienie takie dołączane jest także do akt osobowych pracownika.
7. Każde udostępnienie lub przekazanie akt lub ich kopii innym instytucjom, które z racji wykonywania zadań nałożonych przez stosowne przepisy prawa mogą żądać udostępnienia lub przekazania informacji, musi być odnotowane w *Rejestrze udostępniania danych osobowych przez Urząd Miejski w Brusach*.
8. Udostępnianie danych osobowych do przetwarzania innym instytucjom niż tym, o których mowa w pkt. 7 musi odbywać się przy zachowaniu szczególnych środków ostrożności, które uniemożliwiają osobom nieupoważnionym dostęp do przetwarzanych danych.
9. Zwrot akt lub ich kopii musi zostać odnotowany w *Rejestrze udostępniania danych osobowych przez Urząd Miejski w Brusach*. Zwrócone kopie akt podlegają takiej samej ochronie, jak ich oryginały lub muszą zostać zniszczone.
10. *Rejestr udostępniania danych osobowych przez Urząd Miejski w Brusach* prowadzi Administrator Bezpieczeństwa Informacji urzędu.
11. Jako zbiory danych w postaci tradycyjnej traktowane są również wszelkiego rodzaju wydruki (wykonane przy wykorzystaniu lub bez wykorzystania systemów informatycznych) oraz dokumenty sporządzane odręcznie, jeśli zawierają dane osobowe.
12. Dostęp do akt zawierających dane osobowe mogą mieć tylko osoby upoważnione do przetwarzania danych osobowych przez Administratora Danych Osobowych.
13. Każdy pracownik jest odpowiedzialny za zapewnienie bezpieczeństwa przetwarzanych danych w zakresie oznaczonym ogólnie obowiązującymi regulacjami prawnymi i regulacjami wewnętrznymi urzędu.

III. Zbiory danych w postaci elektronicznej.

1. Systemy informatyczne, w których przechowywane są dane osobowe w postaci elektronicznej podlegają ochronie.
2. Na poziomie systemu operacyjnego i stosowanego oprogramowania ochronie podlegają zbiory danych i wszelkie zbiory pomocnicze generowane przez systemy.
3. Takiej samej ochronie podlegają kopie danych wykonane jako kopie zapasowe i awaryjne.
4. Ochronie podlegają wydruki i inne dokumenty wytworzone przy wykorzystaniu systemów informatycznych.




5. Dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, magnetycznych, optycznych i innych nośników informacji oraz kopii zapasowych i awaryjnych zawierających dane osobowe mogą mieć tylko osoby upoważnione przez Administratora Danych Osobowych.
6. Administrator Bezpieczeństwa Informacji prowadzi *Rejestr upoważnień do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach* zawierający informacje o pracownikach będących użytkownikami systemów, w których przetwarzane są dane osobowe oraz okresie ważności upoważnienia do przetwarzania danych osobowych w systemie informatycznym. Upoważnienie takie dołączane jest także do akt osobowych pracownika.
7. Wszystkie nośniki wykorzystane do kopiowania danych w celach archiwizacji, wymiany lub przeniesienia danych po wykorzystaniu zgodnie z przeznaczeniem muszą zostać zabezpieczone przez odczytem przez osoby nieupoważnione.
8. Identyfikatory użytkowników muszą być unikalne, w powiązaniu z hasłem jednoznacznie identyfikować każdego użytkownika w każdym systemie informatycznym oraz uwzględniać osoby już niepracujące.
9. Hasła użytkowników są poufne i nie mogą być udostępniane innym pracownikom ani osobom nieupoważnionym.
10. Użytkownik systemu informatycznego jest odpowiedzialny za zapewnienie bezpieczeństwa przetwarzanych danych w zakresie oznaczonym ogólnie obowiązującymi regulacjami prawnymi i regulacjami wewnętrznymi urzędu.

§ 4

IV. Osoby odpowiedzialne.

1. Za przetwarzanie informacji odpowiedzialni są:
 - a) Administrator Bezpieczeństwa Informacji,
 - b) Administrator Systemu Informatycznego,
 - c) pracownicy mający bezpośredni dostęp do zbiorów danych lub uczestniczący w ich przetwarzaniu.
2. Zarówno w przypadku zbiorów tradycyjnych jak i w postaci elektronicznej szczególna odpowiedzialność spoczywa na osobach nadzorujących te akta oraz mających do nich bezpośredni dostęp.
3. Instytucje współpracujące z urzędem na podstawie zawartych umów, a mające dostęp do zbiorów danych, winny być poinformowane o odpowiedzialności wynikającej z ustawy. W umowach z nimi powinny znaleźć się klauzule gwarantujące przestrzeganie tej ustawy i rozporządzenia.

BURMISTRZ

mgr inż. Witold Lisowski