

ZARZĄDZENIE NR 35/2016
Starosty Bielskiego
z dnia 1 lipca 2016 roku

w sprawie: ochrony danych osobowych w Starostwie Powiatowym w Bielsku-Białej.

Na podstawie art. 34 ust. 1 oraz art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (t.j. Dz. U. z 2016 roku, poz. 814), art. 36 ust. 1 i 2 oraz 36a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2016 roku, poz. 922)

zarządzam, co następuje:

Rozdział I
Postanowienia ogólne

§ 1

Zarządzenie określa podział odpowiedzialności, zadań i kompetencji w zakresie ochrony danych osobowych w Starostwie Powiatowym w Bielsku-Białej, tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z obowiązującymi przepisami, zasady rejestracji zbiorów danych osobowych i nadawania uprawnień.

§ 2

Przyjęte w zarządzeniu określenia oznaczają:

1. ustawa – ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
2. Administrator Danych Osobowych w Starostwie Powiatowym w Bielsku-Białej - Starostę Bielskiego - zwanego dalej ADO,
3. Administrator Bezpieczeństwa Informacji - osobę wskazaną przez ADO nadzorującą całokształt zagadnień związanych z ochroną danych osobowych w Starostwie Powiatowym w Bielsku-Białej – zwaną dalej ABI,
4. Administrator Systemu Informatycznego - osobę wskazaną przez ADO odpowiedzialną za funkcjonowanie systemów informatycznych w Starostwie Powiatowym w Bielsku-Białej – zwaną dalej ASI,
5. Urząd - Starostwo Powiatowe w Bielsku-Białej,
6. GODO - Generalny Inspektor Ochrony Danych Osobowych.

§ 3

Zarządzenie stosuje się do przetwarzania danych osobowych w systemach informatycznych oraz kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych komórek organizacyjnych Urzędu.

Rozdział II

Odpowiedzialność, zadania i kompetencje

§ 4

W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w Urzędzie ADO powołuje ABI.

§ 5

ABI odpowiada za:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
 - a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych (na wezwanie GIODO, cyklicznych oraz doraźnych),
 - b) nadzorowanie opracowania i aktualizowania dokumentacji - instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i Polityki Bezpieczeństwa oraz przestrzegania zasad w nich zawartych,
 - c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
 - d) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, zgodnie z obowiązującymi przepisami.
2. nadzór nad bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych,
3. nadzór nad przestrzeganiem przez pracowników zasad ochrony danych osobowych obowiązujących w urzędzie,
4. nadzór nad przeprowadzaniem w bezpieczny sposób napraw i konserwacji sprzętu i oprogramowania służącego do przetwarzania danych osobowych lub będącego nośnikiem danych osobowych,
5. nadzór nad nadawaniem i odbieraniem uprawnień do systemów informatycznych, na wniosek osób upoważnionych do wnioskowania o uprawnienia,
6. koordynację procesu reagowania na naruszenia lub próby naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych,
7. organizowanie szkoleń z zakresu ochrony danych osobowych,
8. monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych przetwarzanych w systemach informatycznych, dopasowywanie systemu do wymogów prawnych, tworzenie wewnętrznych unormowań (zarządzeń) w tym zakresie,
9. monitorowanie zaleceń i interpretacji GIODO w zakresie ochrony danych osobowych i rozpowszechnianie ich w urzędzie,
10. przygotowywanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

§ 6

ABI realizując zadania w zakresie ochrony danych osobowych podlega bezpośrednio ADO.

§ 7

Do pomocy przy realizacji zadań określonych w § 5 powołuje się Zastępcę ABI.

§ 8

1. W celu zabezpieczenia funkcjonowania sieci informatycznej, systemów informatycznych oraz sprzętu informatycznego w Urzędzie powołuje się ASI.
2. ASI jest odpowiedzialny za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób nieuprawnionych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń zabezpieczeń w systemie.
3. ASI wykonuje następujące zadania:
 - a) współpracuje z ABI w zakresie ochrony danych osobowych w systemach informatycznych Urzędu,
 - b) wykonuje postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
 - c) tworzy i nadzoruje mechanizm kontroli przetwarzania danych w systemach informatycznych Urzędu,
 - d) określa sposób przepływu danych pomiędzy poszczególnymi systemami,
 - e) określa środki techniczne niezbędne do zapewnienia poufności i integralności przetwarzanych danych,
 - f) odpowiada za właściwe zabezpieczenie kopii zapasowych,
 - g) podejmuje odpowiednie działania w przypadku wykrycia naruszeń w systemie zabezpieczeń,
 - h) analizuje pracę systemów informatycznych przetwarzających dane osobowe w celu wykrycia potencjalnych zagrożeń dla przetwarzania danych,
 - i) nadzoruje proces monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych,
 - j) dopuszcza do eksploatacji nowy system informatyczny do przetwarzania danych osobowych,
 - k) szkoli osoby przyjmowane do pracy w Urzędzie na stanowiska związane z obsługą systemów informatycznych służących do przetwarzania danych osobowych,
 - l) zabezpiecza urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilanych energią elektryczną, przed utratą tych danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 9

1. Za przestrzeganie w komórkach organizacyjnych Urzędu przepisów ustawy odpowiadają kierownicy tych komórek.
2. Do obowiązków kierowników komórek organizacyjnych należy w szczególności:
 - a) wykonywanie zaleceń ABI w zakresie ochrony danych osobowych w systemach informatycznych im podległych,
 - b) wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w podległej komórce organizacyjnej,
 - c) zidentyfikowanie w zasobach podległej jednostki organizacyjnej zbiorów danych osobowych,
 - d) poinformowanie ABI o potrzebie rejestracji zbiorów danych osobowych zidentyfikowanych w podległej komórce organizacyjnej, aktualizacja informacji zawartych w zbiorach danych osobowych, poprzez sporządzanie wniosków o rejestrację / aktualizację zbiorów danych osobowych,
 - e) występowanie do ABI z wnioskiem o upoważnienie osób do pracy przy przetwarzaniu danych osobowych na zasadach zawartych w niniejszym zarządzeniu,
 - f) występowanie z wnioskiem o aktualizację, wycofanie upoważnienia do przetwarzania danych osobowych,
 - g) zapoznanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
 - h) stały nadzór nad przetwarzaniem danych osobowych w podległej sobie komórce organizacyjnej, w szczególności nad zabezpieczeniem danych osobowych przed dostępem osób nieupoważnionych, przejęciem przez osobę nieuprawnioną, uszkodzeniem i zniszczeniem,
 - i) zgłaszanie do ABI potrzeb w zakresie szkoleń podległych pracowników,
 - j) składanie wyjaśnień podczas prowadzonego w komórce organizacyjnej sprawdzenia zgodności przetwarzania danych osobowych z obowiązującymi w tym zakresie przepisami.

§ 10

Pracownicy Urzędu, upoważnieni do przetwarzania danych osobowych są zobowiązani do:

1. ścisłego przestrzegania przepisów o ochronie danych osobowych, w tym zaleceń zawartych w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i Polityki Bezpieczeństwa obowiązującej w urzędzie,
2. zachowania w tajemnicy danych osobowych do których przetwarzania zostali upoważnieni oraz sposobów ich zabezpieczenia,
3. zmiany nie rzadziej niż co 30 dni hasła uwierzytelniającego użytkownika przetwarzającego dane w systemie informatycznym,

4. szczególnej ochrony miejsca przetwarzania danych przed dostępem osób nieupoważnionych w celu uniknięcia zainstalowania oprogramowania, które spowoduje przejęcie przez osobę nieuprawnioną danych służących uwierzytelnieniu (identyfikatora i hasła) lub podłączenia w tym celu w sposób niezauważony odpowiednich urządzeń nazywanych keyloggerami,
5. dopilnowania aby ekran monitora stanowiska informatycznego wykorzystywanego do przetwarzania danych osobowych był ustawiony w sposób uniemożliwiający wgląd do niego osobom do tego nieuprawnionym,
6. dopilnowania aby włączone stacje komputerowe w czasie nieobecności na stanowisku pracy były odpowiednio zablokowane przed dostępem osób nieuprawnionych,
7. każdorazowego zamykania pomieszczeń służbowych, w przypadku czasowego opuszczenia stanowiska pracy, w których przetwarzane są w formie papierowej dane osobowe i nie pozostawiania w nich osób nieuprawnionych, w celu uniemożliwienia wglądu do tych danych albo ich zabrania,
8. po zakończeniu pracy usunięcia z biurk dokumentów zawierających dane osobowe i zabezpieczenie ich przed dostępem osób nieuprawnionych,
9. wykonywania kopii zapasowych zbiorów przetwarzanych danych lokalnie,
10. zgłaszania kierownikowi komórki organizacyjnej wszelkich awarii, uszkodzeń sprzętu informatycznego, za pomocą którego są przetwarzane dane osobowe,
11. udziału w organizowanych szkoleniach z zakresu ochrony danych osobowych.

Rozdział III

Tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z obowiązującymi przepisami

§ 11

Sprawdzenie, o którym mowa w § 5 pkt 1 lit a części II, przeprowadzane jest w trybie:

- a) sprawdzenia planowanego - według planu sprawdzeń,
- b) sprawdzenia doraźnego, w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez ABI wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takich naruszeń,
- c) art. 19 b ust. 1 ustawy - w przypadku zwrócenia się o dokonanie sprawdzenia przez GIODO.

§ 12

Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.

§ 13

ABI w planie sprawdzeń uwzględnia w szczególności zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:

- a) z zasadami przetwarzania danych osobowych, o których mowa w ustawie,
- b) z zasadami dotyczącymi zabezpieczania danych osobowych, o których mowa w ustawie,
- c) z zasadami przekazywania danych osobowych, o których mowa w ustawie, z obowiązkiem zgłaszania zbioru danych osobowych do rejestracji i jego aktualizacji, o których mowa w ustawie.

§ 14

1. Plan sprawdzeń jest przygotowany przez ABI na okres jednego roku kalendarzowego.
2. Plan sprawdzeń jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.

§ 15

Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez ABI o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

§ 16

ABI zawiadamia ADO o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia w trybie, o którym mowa w art. 19 b ust. 1 ustawy, przed podjęciem pierwszej czynności w toku sprawdzania.

§ 17

ABI dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

§ 18

Dokumentowanie czynności w toku sprawdzenia może polegać w szczególności na realizacji zadań określonych w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015r., poz. 745).

§ 19

W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności ABI mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności osoby zarządzającej tym systemem.

§ 20

Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia ABI przeprowadzenie czynności w toku sprawdzenia.

§ 21

ABI zawiadamia kierownika komórki organizacyjnej o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

§ 22

Zawiadomienia nie przekazuje się w przypadku:

- a) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce,
- b) sprawdzenia, o którego dokonanie zwrócił się GIODO, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin,
- c) jeżeli kierownik komórki organizacyjnej posiada informacje, o których mowa w ust. b.

§ 23

Do wykonywania czynności realizowanych w toku sprawdzenia ABI może korzystać z pomocy powołanego Zarządzeniem Starosty Bielskiego Zespołu Auditorów Wewnętrznych Systemu Zarządzania Jakością i Bezpieczeństwem Informacji zgodnego z wymaganiami normy ISO 9001 i ISO 27001.

§ 24

Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie (w wersji papierowej lub elektronicznej).

§ 25

ABI przekazuje ADO sprawozdanie:

- a) ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia,
- b) ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia,
- c) ze sprawdzenia, o którego dokonanie zwrócił się GIODO – zachowując termin wskazany przez GIODO zgodnie z art. 19 b ust. 1 ustawy.

Rozdział IV

Rejestracja zbiorów danych osobowych

§ 26

1. Zgłoszeniu do rejestracji GIODO podlegają zbiory zawierające dane, o których mowa w art. 27 ust. 1 ustawy.
2. Wzór wniosku o rejestrację zbiorów danych osobowych, o których mowa w § 26 pkt 1 niniejszego zarządzenia, został określony w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 roku w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. Nr 229, poz.1536).
3. Wpis nowego zbioru do rejestru zbiorów danych osobowych przetwarzanych w urzędzie jest dokonywany na podstawie pisemnego wniosku stanowiącego załącznik Nr 1 do niniejszego zarządzenia.
4. Informacje zawarte w rejestrze zbiorów danych osobowych przetwarzanych w urzędzie oraz sposób udostępniania rejestru określa rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r. , poz. 719).
5. Wnioski o zgłoszenie do rejestracji GIODO oraz wpis nowego zbioru do rejestru zbiorów danych osobowych przetwarzanych w urzędzie są przekazywane do ABI w wersji papierowej lub elektronicznej.

§ 27

Zwolnienie z obowiązku zgłoszenia zbioru danych osobowych do rejestracji GIODO, które dotyczy zbiorów wskazanych w art. 43 ust. 1 ustawy, nie zwalnia użytkowników danych od zabezpieczenia ich przed nieuprawnionym dostępem lub utratą.

Rozdział V

Nadawanie uprawnień

§ 28

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby upoważnione.
2. Upoważnienia do przetwarzania danych osobowych w Starostwie Powiatowym w Bielsku-Białej nadaje ADO.
3. Kierownicy komórek organizacyjnych urzędu występują pisemnie o upoważnienie pracowników lub innej osoby (np. stażysty, praktykanta) do przetwarzania danych osobowych.
4. Wzór wniosku o przygotowanie upoważnienia do przetwarzania danych osobowych stanowi Załącznik Nr 2 do niniejszego zarządzenia.
5. Upoważnienie do przetwarzania danych osobowych przygotowywane jest w 3 egzemplarzach.

6. Wzór upoważnienia stanowi Załącznik Nr 3 do niniejszego zarządzenia.
7. Rejestr osób upoważnionych do przetwarzania danych osobowych w urzędzie prowadzony jest w formie elektronicznej.
8. Kierownicy komórek organizacyjnych mają wgląd do rejestru elektronicznego oraz dokonują bieżącej weryfikacji zapisów w rejestrze.
9. W przypadku wystąpienia konieczności aktualizacji lub wycofania upoważnienia obowiązuje wzór wniosku stanowiący Załącznik Nr 2 do niniejszego zarządzenia.
10. W przypadku rozwiązania stosunku pracy z pracownikiem upoważnionym traci moc upoważnienie.
11. ASI w przypadku rozwiązania umowy blokuje konto użytkownika w systemach informatycznych.

Rozdział VI

Postanowienia końcowe

§ 29

W sprawach nieuregulowanych w niniejszym zarządzeniu mają zastosowanie przepisy ustawy oraz wydanej na jej podstawie akty wykonawcze.

§ 30

Wykonanie zarządzenia powierzam kierownikom komórek organizacyjnych.

§ 31

Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Powiatu.

§ 32

Traci moc Zarządzenie Nr 83/2015 Starosty Bielskiego z dnia 30 grudnia 2015 roku w sprawie: ochrony danych osobowych w Starostwie Powiatowym w Bielsku-Białej oraz Zarządzenie Nr 16/2006 Starosty Bielskiego z dnia 10 maja 2006 roku w sprawie ustalenia zasad udostępniania bazy ewidencji gruntów i budynków Wydziałom Starostwa Powiatowego w Bielsku-Białej.

§ 33

Zarządzenie wchodzi w życie z dniem podpisania.