

ZARZĄDZENIE Nr 51/2015
Burmistrza Bornego Sulinowa
z dnia 21 maja 2015 r.

w sprawie wyznaczenia i określenia zadań Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miejskim w Bornem Sulinowie

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2014 r., poz. 594 z późn. zm.) w związku z art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) **zarządzam**, co następuje:

§ 1. 1. Wyznaczam Pana Wiesława Fabisińskiego na Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Bornem Sulinowie.

2. Ustalam zakres zadań i uprawnień Administratora Bezpieczeństwa Informacji, stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2. 1. Wyznaczam Pana Kacpra Kobyłeckiego na Administratora Systemu Informatycznego w Urzędzie Miejskim w Bornem Sulinowie.

2. Ustalam zakres zadań Administratora Systemu Informatycznego, stanowiący załącznik nr 2 do niniejszego zarządzenia.

§ 3. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 4. Traci moc zarządzenie nr 20/2013 Burmistrza Bornego Sulinowa z dnia 18 lutego 2013 r. w sprawie wyznaczenia i określenia zadań Administratora Bezpieczeństwa Informacji i Administratora Systemów Informatycznych w Urzędzie Miejskim w Bornem Sulinowie.

§ 5. Zarządzenie wchodzi w życie z dniem 31 maja 2015 r.

Zakres zadań i uprawnienia Administratora Bezpieczeństwa Informacji

1. Administrator Bezpieczeństwa Informacji (ABI) podlega bezpośrednio Administratorowi Danych Osobowych (ADO) w Urzędzie Miejskim.

2. ABI podczas wykonywania zadań wynikających z niniejszego zakresu współpracuje z Administratorem Systemu Informatycznego (ASI) oraz kierownikami referatów i pracownikami na samodzielnych stanowiskach pracy.

3. Celem działania ABI jest zachowanie bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim poprzez nadzorowanie i sprawdzanie przestrzegania zasad ochrony danych osobowych. Zadaniem ABI jest realizacja przedsięwzięć określonych art. 36a ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2014 r., poz. 1182), a w szczególności:

1) zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO,

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 oraz przestrzegania zasad w niej określonych,

c) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje o których mowa w art. 41 ust. 1 pkt 2-4a i 7.

4. Do szczegółowych czynności ABI należy:

1) nadzorowanie i kontrolowanie przestrzegania zasad:

a) przetwarzania danych osobowych przez użytkowników zgodnie z zakresem nadanego im upoważnienia,

b) stosowania przez użytkowników ustaleń dotyczących przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania, oraz przechowywania, w tym w systemach informatycznych,

- d) ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń,
- e) wyposażenia oraz zabezpieczenia pomieszczeń, w których przechowuje się dane sensorywne i kopie zapasowe zbiorów,
- f) wprowadzania, przekazywania, i udostępniania danych osobowych we współpracy z właściwymi pracownikami Urzędu Miejskiego.

2) realizowanie zadań w zakresie:

- a) sporządzania sprawozdania dla ADO dotyczącego zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- b) udzielanie pomocy pracownikom Urzędu Miejskiego, rozpatrywania skarg i wniosków dotyczących przetwarzania danych,
- c) tworzenia projektów zarządzeń, instrukcji i wytycznych ADO,
- d) wyjaśniania i dokumentowania przypadków naruszania zasad przetwarzania i ochrony danych osobowych w Urzędzie Miejskim,
- e) organizowania i prowadzenia szkoleń z zakresu przetwarzania danych osobowych,
- f) odnotowywania i dokumentowania zmian w lokalizacji obszarów przetwarzania danych we współpracy z właściwymi pracownikami Urzędu Miejskiego,
- g) wykonywania okresowych analiz zagrożeń bezpieczeństwa i ocen stanu ochrony danych osobowych przetwarzanych w obszarach,
- h) prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych,
- i) prowadzenia rejestru zbioru danych osobowych w Urzędzie Miejskim,
- j) zgłaszania zbiorów zawierających dane sensorywne w Biurze Generalnego Inspektora Ochrony Danych Osobowych (GIODO) lub zmian w przetwarzaniu danych osobowych w zbiorach zgłoszonych do rejestracji w GIODO, we współpracy z właściwymi pracownikami Urzędu Miejskiego,
- k) prowadzenia i aktualizacji dokumentacji w zakresie przetwarzania danych osobowych.

5. Wykonując swoje czynności ABI działa w imieniu ADO i posiada uprawnienia do:

- 1) wskazywania zastosowania odpowiednich zabezpieczeń technicznych i wykonywania czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych,

- 2) parafowania umów dotyczących udostępniania lub powierzenia danych do przetwarzania osobom lub podmiotom zewnętrznym w zakresie stosowania w nich zapisów dotyczących bezpieczeństwa przetwarzania osobowych,
- 3) wnioskowania o ograniczenie zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia dla bezpieczeństwa i ochrony danych osobowych,
- 4) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie sprawdzania i dostosowania ochrony danych do stanu zgodnego z przepisami prawa,
- 5) zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych,
- 6) wydawania w imieniu ADO upoważnień osobom do przetwarzania danych osobowych.

Zakres zadań Administratora Systemu Informatycznego.

Administrator Systemu Informatycznego (ASI), wykonuje zadania w zakresie nadzorowania zasad ochrony danych osobowych, w tym wynikających z Instrukcji bezpieczeństwa systemów informatycznych, a w szczególności:

- 1) nadawanie identyfikatorów użytkownikom danych osobowych,
- 2) zabezpieczenie i kontrolowanie prawidłowości przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,
- 3) pozbawianie zapisu danych osobowych lub uszkodzanie w sposób uniemożliwiający odczytanie urządzeń lub nośników, które przeznaczone są do likwidacji,
- 4) instalowanie zabezpieczeń w systemach informatycznych,
- 5) wyrejestrowywanie i rejestrowanie z systemu użytkowników w czasie instalowania oraz modyfikacji systemu,
- 6) przydzielanie uprawnień do poszczególnych systemów,
- 7) wykonywanie kopii awaryjnych danych z serwera, właściwe przechowywanie nośników, sprawdzanie poprawności zapisu oraz ich likwidowanie,
- 8) dokonywanie wyboru lub migracji do technologii minimalizującej zagrożenia uzyskania dostępu do sieci osobom nieupoważnionym,
- 9) nadzorowanie procesu monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych,
- 10) wykonywanie poleceń Administratora Bezpieczeństwa Informacji w zakresie zarządzania podległymi systemami informatycznymi,
- 11) czuwanie nad właściwym eksploataowaniem podległych mu systemów informatycznych,
- 12) stwarzanie właściwych warunków organizacyjno-technicznych gwarantujących bezpieczeństwo podległych mu systemów informatycznych,
- 13) nadzorowanie właściwej lokalizacji sprzętu komputerowego, tj. ustawiania monitorów i drukarek uniemożliwiającego wgląd w dane osobowe osobom nieupoważnionym lub kradzież wymiennych nośników danych,
- 14) występowanie do Administratora Danych Osobowych z wnioskiem o upoważnienie pracowników do przetwarzania danych osobowych,

15) nadawanie haseł dostępu użytkownikom oraz ustawianie uprawnień w podległych im systemach,

16) pozbawianie zapisu danych osobowych z nośników, które przeznaczone są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych,

17) prowadzenie, uaktualnianie na bieżąco oraz przesyłanie Administratorowi Bezpieczeństwa Informacji danych dotyczących:

a) listy użytkowników danych osobowych wraz z przydzielonymi im uprawnieniami do poszczególnych funkcji systemu,

b) lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku jakichkolwiek zmian tych danych,

c) rodzaju systemów informatycznych funkcjonujących w zakresie ich działania,

d) czynności serwisowych wykonywanych w podległych systemach informatycznych,

e) zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytych wirusów, koni trojańskich itp. oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania,

18) zgłaszanie Administratorowi Bezpieczeństwa Informacji potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych.

Ponadto uczestniczy w zespołach prowadzących sprawdzenie przestrzegania zasad ochrony danych osobowych przetwarzanych w Urzędzie Miejskim.