Załącznik Nr 1 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta Szczecin

§ 1. Organizacja Systemu Zarządzenia Bezpieczeństwem Informacji (Pkt 6.1*)

1. Kierownicy odpowiadają za:

1) przeszkolenie instruktażowe pracowników w zakresie związanym z bezpieczeństwem informacji na stanowiskach pracy,

2) przestrzeganie zasad bezpieczeństwa informacji przez nich samych jak i przez podległych im pracowników,

3) identyfikowanie i dokumentowanie zagrożeń istotnych dla bezpieczeństwa informacji.

2. Zobowiązuje się kierowników sporządzających projekty umów do zawierania w nich wymagań ochrony danych osobowych oraz bezpieczeństwa informacji w stopniu właściwym do zakresu umowy, a następnie ich przedkładania celem ostatecznej weryfikacji (akceptacji) oraz zaparafowania do ABI.

3. Odpowiedzialność za bezpieczeństwo informacji w Urzędzie ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków oraz uregulowaniami wewnętrznymi w przedmiotowej sprawie.

4. Każdy pracownik jest obowiązany dbać o bezpieczeństwo powierzonych mu do przetwarzania danych osobowych/informacji, zgodnie z obowiązującymi przepisami wewnętrznymi, w tym w szczególności:

1) stosować zasady opisane w niniejszej PBI oraz innych dokumentach wewnętrznych, mających znaczenie z punktu widzenia bezpieczeństwa informacji,

2) chronić informacje istotne z punktu widzenia bezpieczeństwa informacji przed dostępem do nich osób nieuprawnionych, przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,

3) stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z SZBI.

§ 2. Podstawowe obowiązki w obszarze zarządzania bezpieczeństwem informacji (A.6.1.2*):

1. Administrator Danych Osobowych Urzędu (AD):

1) zatwierdza warunki techniczne i organizacyjne służące bezpieczeństwu informacji, w tym ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

2) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony informacji, w tym danych osobowych,

3) odpowiada za zgodne z prawem przetwarzanie informacji, w tym zasad obrotu i zabezpieczenia danych osobowych.

2. Administrator Bezpieczeństwa Informacji (ABI):

1) zapewniania przestrzeganie przepisów o ochronie danych osobowych, w szczególności przez, sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

2) opracowuje w tym zakresie sprawozdania dla AD, nadzoruje opracowanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2 ustawy oraz nadzoruje przestrzeganie zasad w niej określonych,

3) zapewniania zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

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

3. Administrator Systemu Informatycznego (ASI) (A 9.1, A 9.2*):

1) odpowiada za bezpieczeństwo, rozliczalność, niezaprzeczalność oraz integralność danych zgromadzonych w zbiorach danych za pomocą systemów informatycznych,

2) zarządza bezpieczeństwem informacji, w tym ochroną danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI,

3) przygotowuje projekty, opisy przedmiotu zamówienia w przypadku planowanych zakupów urządzeń wsparcia wydajności systemu informatycznego,

4) przydziela identyfikatory (loginy) użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,

5) prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne

6) zarządza kopiami awaryjnymi danych, w tym danych osobowych,

4. Administrator Systemu Użytkowego (ASU) (A.9.2*)

1) nadaje, aktualizuje i odbiera uprawnienia do poszczególnych modułów lub funkcji systemu użytkowego,

2) testuje nowe wersje systemu,

3) sprawuje nadzór nad prawidłowym działaniem systemu użytkowego,

4) zgłasza dostawcy systemu uwagi użytkowników oraz nowe funkcjonalności.

5. Użytkownik:

1) odpowiada za poprawność merytoryczną danych gromadzonych w zbiorach danych za pomocą systemów informatycznych,

2) chroni prawo do prywatności osób fizycznych powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w niniejszej PBI, IZSI, IPNBI, PCD,

3) współpracuje z osobami pełniącymi role odpowiedzialne za bezpieczeństwo informacji w SZBI tj. z ABI ASI i ASU w zakresie realizacji zadań dotyczących bezpieczeństwa informacji.

§ 3. 1. AD zapewnia, że wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych, w tym systemów i aplikacji informatycznych własnych i/lub podmiotów zewnętrznych, wykorzystywanych wewnętrznie prowadzone jest w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa informacji. (A.14*)

2. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych obejmuje:

1) uwzględnianie wymogów bezpieczeństwa podczas zakupu lub budowy nowych systemów informatycznych,

2) przeprowadzenie testów funkcjonalnych i testów bezpieczeństwa przed dopuszczeniem nowego systemu do eksploatacji,

3) nadzorowanie dostępu do kodów źródłowych oprogramowania,

4) wdrożenie mechanizmów aktualizacji oprogramowania,

5) wdrożenie procedur kontroli zmian oprogramowania.

3. Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju i utrzymania systemów informacyjnych AD odpowiedzialny jest Dyrektor WInf.

§ 4. 1. Zarządzanie zdarzeniami i incydentami odbywa się w ramach procesu zarządzania oraz minimalizowania ryzyka wystąpienia incydentów. (A.16.1*)

2. Każdy zauważony incydent lub zdarzenie powinno zostać zgłoszone do ABI i zarejestrowane przez niego, zgodnie z uregulowaniami Instrukcji Postępowania w Sytuacji Naruszenia Bezpieczeństwa Informacji obowiązującej w Urzędzie - IPNBI.

§ 5. AD dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem informacji. (A.17*)

§ 6. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowi **Załącznik nr 3** do zarządzenia.

§ 7. 1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych jest dostępny na żądanie u ABI.

2. Na zbiory danych osobowych w Urzędzie składają się:

1) dane w formie dokumentacji papierowej (wykazy, listy, korespondencja, wnioski, deklaracje, wydruki komputerowe, itp.),

2) dane przetwarzane i przechowywane w systemach informatycznych oraz nośniki z tymi danymi.

2. Kierownicy, przed przystąpieniem do przetwarzania zbiorów danych osobowych lub zakładający takie zbiory są zobowiązani na bieżąco zgłaszać do ABI lub za jego pośrednictwem do Generalnego Inspektora Ochrony Danych Osobowych (GIODO), następujące procesy:

1) zamiar założenia zbioru danych osobowych (zbioru);

2) rozpoczęcie pracy ze zbiorem;

3) każdą modyfikację lub zmianę sposobu wykorzystywania zbioru;

4) fakt zaprzestania eksploatacji zbioru;

5) konieczność likwidacji i sposób likwidacji zbioru.

3. Kierownicy zobowiązani są do:

1) wypełnienia i przekazywania do ABI druku zgłoszenia zbioru danych osobowych według wzoru stanowiącego załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych;

2) przekazywania do ABI opisów struktur zbiorów danych osobowych przetwarzanych w systemach informatycznych z uwzględnieniem i wskazaniem przepływu danych osobowych do innych systemów informatycznych;

3) przekazywania na bieżąco do ABI informacji o zmianach występujących w sposobie przetwarzania zbioru danych osobowych lub zmianie struktury tych zbiorów.

4. ABI prowadzi rejestr zbiorów danych przetwarzanych przez AD oraz ewidencję zbiorów zgłoszonych do GIODO.

5. ABI przekazuje zgłoszenia zbiorów danych osobowych do GIODO zgodnie z przyjętymi w Urzędzie procedurami.

6. Rejestr zbiorów danych osobowych prowadzony jest przez ABI w formie elektronicznej oraz udostępniany jest w Biuletynie Informacji Publicznej Urzędu. Ewidencja opisów struktur zbiorów danych osobowych przetwarzanych w systemach informatycznych i przepływu danych osobowych do innych systemów prowadzona jest przez ASU.

§ 8. Opis struktur zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi jest dostępny w dedykowanym zasobie informatycznym.

§ 9. Zabezpieczenie budynków, pomieszczeń lub części pomieszczeń (A.11.1*)