Burmistrz Złotego Stoku

ZARZĄDZENIE Nr 214 /2016
Burmistrza Złotego Stoku

z dnia 19 stycznia 2016 r.

w sprawie wprowadzenia
Instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Miejskim w Złotym Stoku

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r. poz. 2135 z późn. zm.) i § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1. Wprowadzam Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Złotym Stoku, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuję sekretarza gminy oraz administratora bezpieczeństwa informacji do zapoznania pracowników z zakresem stosowania Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Złotym Stoku najpóźniej do 5 lutego 2016 r.

§ 3. Zobowiązuję wszystkich pracowników do przestrzegania zasad zawartych w zarządzeniu.

§ 4. Wykonanie zarządzenia powierzam sekretarzowi gminy.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Grażyna Orczyk

Załącznik do zarządzenia Nr 214/2016
Burmistrza Złotego Stoku
z dnia 29 stycznia 2016 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Złotym Stoku

§ 1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Złotym Stoku, zwana dalej instrukcją, określa sposób zarządzania oraz zasady administrowania systemem informatycznym, w którym przetwarzane są dane osobowe.

§ 2. Użyte w treści instrukcji określenia oznaczają:

1) urząd – Urząd Miejski w Złotym Stoku;
2) ustawa – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
3) rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
4) administrator danych osobowych – Burmistrza Złotego Stoku decydującego o celach i środkach przetwarzania danych osobowych;
5) administrator bezpieczeństwa informacji – osobę funkcyjną wyznaczaną przez administratora danych osobowych, odpowiedzialną za przestrzeganie zasad ochrony danych osobowych i nadzorującą bezpieczeństwo przetwarzania danych osobowych w urzędzie;
6) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
7) użytkownik – osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8) kopii pełnej – należy przez to rozumieć kopię zapasową całości danych osobowych przetwarzanych w systemie informatycznym;
9) polityce bezpieczeństwa – Politykę bezpieczeństwa danych osobowych w Urzędzie Miejskim w Złotym Stoku.
10) sieć publiczna – publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

§ 3. 1. Administrator bezpieczeństwa informacji jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym stosowanym w urzędzie.

2. Do obowiązków administratora bezpieczeństwa informacji należy także:

1) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego;
2) zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

§ 4. Uwzględniając fakt, że użytkowany w urzędzie system informatyczny jest połączony z siecią publiczną, wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

§ 5. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania uprawnień w systemie informatycznym określa się w następujący sposób:

1) użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia oraz po podpisaniu oświadczenia, stanowiących załączniki do polityki bezpieczeństwa, składa ustnie wniosek do administratora bezpieczeństwa informacji o nadanie identyfikatora i hasła w celu umożliwienia wykonywania przetwarzania danych osobowych w systemie informatycznym;
2) administrator bezpieczeństwa informacji zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i hasło w sposób uniemożliwiający zapoznanie się z nim osobom trzecim;
3) w przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, administrator bezpieczeństwa informacji zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.

§ 6. Stosuje się następujące metody oraz środki uwierzytelniania:

1) hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
2) osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest administrator bezpieczeństwa informacji;
3) użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła, jest również zobowiązany do zmiany hasła, co każde 30 dni;
4) użytkownik jest odpowiedzialny za zachowanie poufności swojego hasła.

§ 7. Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

1) w celu zalogowania do systemu informatycznego użytkownik podaje swój identyfikator oraz hasło;
2) system jest skonfigurowany w taki sposób, aby po okresie 5 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu identyfikatora i hasła;
3) po zakończeniu pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera.

§ 8. Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania:

1) raz na miesiąc administrator bezpieczeństwa informacji wykonuje kopię przyrostową;
2) raz na rok administrator bezpieczeństwa informacji wykonuje kopię pełną;
3) wykonane kopie zapasowe przechowuje się na pamięci przenośnej (*pendrive*) lub na nośnikach CD\DVD, nośniki zawierające kopie zapasowe są przechowywane w szafie zamykanej na klucz.

§ 9. 1. Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są w szafach zamykanych na klucz, do których dostęp ma jedynie administrator danych osobowych oraz administrator bezpieczeństwa informacji.

2. Dane osobowe są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania, po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.

3. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe zabezpieczany jest zgodnie z zasadami opisanymi w polityce bezpieczeństwa.

§ 10. System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania:

1) oprogramowaniem antywirusowym stosowanym w urzędzie jest Kaspersky Endpoint Security;
2) zabezpieczenie sprzętowe UTM FortiGate 60C.

§ 11. Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemu informatycznego oraz nośników informacji służących do przetwarzania danych:

1) administrator bezpieczeństwa informacji raz na 3 miesiące wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu

poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z instrukcji;

2) w przypadku stwierdzenia przez administratora bezpieczeństwa informacji nieprawidłowości w działaniu elementów systemu informatycznego podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania;

§ 12. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie zasilaczy awaryjnych UPS, połączonych pomiędzy siecią zasilającą a komputerami oraz listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami.

§ 13. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym dodatkowo zabezpiecza hasłem pliki lub foldery zawierające dane osobowe.

§ 14. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem administrator bezpieczeństwa informacji.

§ 15. Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych osobowych (z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie) zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu (automatycznie);
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu (automatycznie);
3) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą);
4) informacji o odbiorcach w rozumieniu ustawy.

§ 16. Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 15.

§ 17. W przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego stosuje się następującą procedurę:

1) w przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń przez osoby nieuprawnione jest on zobowiązany niezwłocznie poinformować o tym fakcie administratora bezpieczeństwa informacji;
2) administrator bezpieczeństwa informacji jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości.

§ 18. 1. Usuwanie danych osobowych utrwalonych na nośnikach elektronicznych następuje poprzez powierzenie tych nośników w celu usunięcia zapisanych na nich danych wyspecjalizowanej w tej dziedzinie firmie informatycznej, lub poprzez nadpisanie usuwanych informacji przez administratora bezpieczeństwa informacji w taki sposób, aby nie istniała możliwość ich ponownego odczytania.

2. W celu usunięcia danych osobowych zapisanych na elektronicznych nośnikach administrator bezpieczeństwa informacji może dokonać ich fizycznego uszkodzenia w taki sposób, aby nie istniała możliwość odtworzenia zapisanych na nich danych osobowych.

§ 19. W sprawach nieuregulowanych niniejszą instrukcją znajdują zastosowanie przepisy ustawy oraz rozporządzenia.

BURMISTRZ
Grażyna Orczyk

.....
podpis administartora danych osobowych