STAROSTA WOŁOMIŃSKI
ul. Prądzyńskiego 3
05-200 WOŁOMIN

WOK-120.170.2016

Wołomin, dnia 16.08.2016r.

ZARZĄDZENIE NR 170.2016
STAROSTY WOŁOMIŃSKIEGO
Z DNIA 16 SIERPNIA 2016R.

w sprawie planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Starostwie Powiatowym w Wołominie

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (t. j. Dz. U. z 2016r. poz. 814) w związku z art. 36a ust. 2 pkt 1 lit a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz.U. 2016r. poz. 922) oraz § 3 ust. 3 i 5 Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku 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. 7745) zarządzam, co następuje:

§ 1

Zatwierdzam plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Starostwie Powiatowym w Wołominie na okres od 1 września 2016 roku do 31 grudnia 2016 roku w brzmieniu załącznika do niniejszego zarządzenia.

§ 2

Powołuję zespół do przeprowadzenia sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Starostwie Powiatowym w Wołominie w składzie:

1) Marzena Bańka – Administrator Bezpieczeństwa Informacji
2) Konrad Pietrykowski – Administrator Systemów Informatycznych, Zastępca Administratora Bezpieczeństwa Informacji.

§ 3

Zobowiązuję zespół do przedstawienia sprawozdania ze sprawdzeń określonych w załączniku po zakończeniu każdego ze sprawdzeń.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Kazimierz Rakowski

Radca Prawny
WA-10459
Monika Dąbrowska

ADMINISTRATOR
Bezpieczeństwa Informacji
Marzena Bańka

Załącznik
do Zarządzenia Nr 170.2016
Starosty Wołomińskiego
z dnia 16.08.2016r.

Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Starostwie Powiatowym w Wołominie

na okres od 1 września 2016 r. do 31 grudnia 2016 r.

Plan sprawdzeń sporządzony na podstawie § 3 ust.2 pkt 1) oraz zgodnie z wytycznymi zawartymi w §3 oraz §4 Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

Przedmiotem sprawdzenia jest zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Starostwie Powiatowym w Wołominie, a w szczególności:
- realizacja procedur wdrożonych przez ADO w zakresie ochrony danych osobowych,
- zasady przechowywania dokumentów zawierających dane osobowe oraz zasady ich zabezpieczania po zakończeniu pracy,
- funkcjonowanie zastosowanych zabezpieczeń fizycznych,
- funkcjonowanie systemów zabezpieczeń systemowych,
- prawidłowość funkcjonowania mechanizmów kontroli dostępu do zbiorów danych osobowych.

Zakres sprawdzeń i ich szczegółowa tematyka:
Etap I. Sprawdzenie dokumentacji:
1. Czy opracowano i wdrożono politykę bezpieczeństwa oraz instrukcję zarządzania systemami informatycznymi.
2. Czy oba dokumenty są zgodne z obowiązującymi przepisami.
3. Czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia.
4. Czy wszystkie osoby, które mają dostęp do danych osobowych zostały zapoznane z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych – oświadczenia.
5. Czy prowadzona jest ewidencja upoważnień.
6. Czy ewidencja jest zgodna z posiadanymi upoważnieniami.

Etap II. Sprawdzenie stanu faktycznego na podstawie obserwacji i wywiadów:
1. Stosowanie w praktyce zasad określonych w polityce bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych, instrukcji zarządzania systemem informatycznym, w zasadach korzystania z komputerów służbowych oraz ochrony własności intelektualnej.
2. Ustawienie sprzętu komputerowego w pomieszczeniach – czy umożliwia dostęp do ekranu monitorów osobom postronnym.

3. Zabezpieczenie dokumentów zawierających dane osobowe (czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym).
4. Przestrzeganie przez pracowników procedur związanych z zabezpieczeniem danych w trakcie pracy – na podstawie obserwacji oraz rozmów z nimi.
5. Sposób niszczenia niepotrzebnych dokumentów.
6. Dostęp pracowników do zbiorów danych oraz zakres dostępu pracowników i weryfikacja wydanych upoważnień (w tym byłych pracowników oraz odwołanie upoważnień).
7. Legalność przetwarzania danych osobowych – spełnianie warunków art. 23 ust. 1 ustawy o ochronie danych osobowych.
8. Realizacja obowiązku informacyjnego wynikającego z art. 24 ustawy o ochronie danych osobowych.
9. Respektowanie praw osób, których dane są przetwarzane (rozdział 4 ustawy o ochronie danych osobowych).

Etap III. Sprawdzenie bezpieczeństwa teleinformatycznego. Porównanie stanu faktycznego z zapisami z instrukcji zarządzania systemami informatycznymi, w szczególności

1. Zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych.
2. Przestrzeganie zasady rozpoczęcia i zakończenia pracy w systemie.
3. Blokowanie systemu podczas opuszczenia stanowiska pracy w czasie dnia pracy.
4. Upoważnienia osób dopuszczonych do pracy w systemie.
5. Stosowanie identyfikatorów i haseł dla użytkowników zgodnie z wymogami formalnymi.
6. Poziom ochrony systemów informatycznych służących do przetwarzania danych osobowych przed osobami trzecimi.
7. Zabezpieczenie systemowe i fizyczne sprzętu komputerowego (np. przed wyniesieniem).
8. Tworzenie kopii zapasowych – czy umożliwiają odzyskanie danych.
9. Odnotowywanie przez systemy służące do przetwarzania danych osobowych czynności wykonywanych na danych osobowych przez użytkowników.
10. Sposób niszczenia lub usuwania danych wygenerowanych z systemów.

Plan sprawdzeń z zakresu ochrony danych osobowych:

Lp.	Termin (rozpoczęcie – zakończenie)	Wydział (Przedmiot)	Zakres	Efekt końcowy
1.	01.09.2016 – 30.09.2016	WSO	Zbiory danych osobowych w wydziale	Raport końcowy* wraz z planem ewentualnych działań naprawczych
2.	01.10.2016 – 31.10.2016	WKM	Zbiory danych osobowych w wydziale	Raport końcowy* wraz z planem ewentualnych działań naprawczych
3.	01.11.2016 – 30.11.2016	WOZ	Zbiory danych osobowych w wydziale	Raport końcowy* wraz z planem ewentualnych działań naprawczych

Zasady dokumentowania czynności:

1. Z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych sporządza się notatkę odpowiednio według załączonych wzorów.

2. W trakcie sprawdzenia można wykonać kopię otrzymanego dokumentu, obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych oraz zapisu rejestru systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.
3. Powyższe dokumenty przechowuje się w formie papierowej oraz elektronicznej.

* Poprzez raport końcowy należy rozumieć sprawozdanie określone w art. 36c ustawy o ochronie danych osobowych.

STAROSTA

Kazimierz Rakowski