

ZARZĄDZENIE NR 16/2017
WÓJTA GMINY PRUSZCZ GDAŃSKI

z dnia 10 lutego 2017r.

w sprawie wprowadzenia „Planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w 2017 roku”

Na podstawie art. 36a ust. 2 pkt 1 lit. a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922) oraz na podstawie § 3 ust 5 Rozporządzenia 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. poz. 745) zarządza się, co następuje:

§ 1. Wprowadza się „Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w 2017 roku”, który stanowi załącznik do zarządzenia.

§ 2. Wykonanie zarządzenia powierza się pracownikowi pełniącemu funkcję administratora bezpieczeństwa informacji w Urzędzie Gminy Pruszcz Gdański.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.


Magdalena Kołodziejczak

PLAN SPRAWDZEŃ ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH W URZĘDZIE GMINY PRUSZCZ GDAŃSKI W 2017 ROKU

I. WSTĘP

1. Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (zwany dalej planem sprawdzeń) opracowany jest na podstawie art. 36a ust. 2 pkt 1 lit. a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych przez administratora bezpieczeństwa informacji zwanego dalej ABI i zatwierdzany jest przez Administratora Danych Osobowych zwanego dalej ADO.

2. ABI w czasie przeprowadzania sprawdzeń ma prawo:

- a) Sporządzać notatki z przeprowadzonych czynności lub otrzymanych wyjaśnień;
- b) Kopiować otrzymane od osoby sprawdzanej dokumenty;
- c) Tworzyć zrzuty ekranu urządzeń na których są przetwarzane lub zabezpieczone dane osobowe;
- d) Sporządzać kopie zapisów rejestru systemu informatycznego służącego do przetwarzania danych osobowych zwanego dalej systemem;
- e) Sporządzać kopie zapisów konfiguracyjnych środków służących do zabezpieczeń systemu.

3. Osoba odpowiedzialna za przetwarzanie danych osobowych w zbiorze danych osobowych lub systemie objętym sprawdzeniem, bierze udział w sprawdzeniu lub umożliwia ABI przeprowadzenie czynności w toku sprawdzenia.

II. ZAKRES SPRAWDZENIA

Sprawdzenie zostanie przeprowadzone w terminie od dnia 24 lutego 2017r. do 29 grudnia 2017r.

1. Sprawdzeniu zgodności przetwarzania danych osobowych podlegają zbiory:

- a) Rejestr Przedpoborowych;
- b) System Windykacji Podatkowej;
- c) Pomoc Materialna dla uczniów;
- d) System Informacji Oświatowej;
- e) Wypisy i wyrisy z miejscowego planu zagospodarowania przestrzennego;
- f) Wydawanie zezwoleń na usunięcie drzew i krzewów. Naliczanie kar za niszczenie i usuwanie drzew i krzewów bez zezwolenia;
- g) Karta Rodziny Wielodzietnej;
- h) Zgłoszenie zbiorników bezodpływowych.

2. Sprawdzeniu podlegają w szczególności:

- a) sprawdzenie podstawy prawnej przetwarzania danych osobowych (Art. 23 ust 1, Art. 27 UODO);
- b) sprawdzenie sposobu dopełnienia obowiązków administratora danych w zakresie:
 - wykonania obowiązku informacyjnego w przypadku zbierania danych osobowych od osoby, której one dotyczą (Art. 24 UODO);
 - wykonania obowiązku informacyjnego w przypadku zbierania danych osobowych z innych źródeł, niż od osoby, której one dotyczą (Art. 25 UODO);
 - realizacji prawa osoby do uzyskania informacji o istnieniu zbioru, ustalenia administratora danych, uzyskania informacji o celu, zakresie, sposobie, czasie, źródle pochodzenia, sposobie udostępniania danych osobowych oraz do żądania aktualizacji/ wstrzymania/ usunięcia danych (Art. 32 ust. 1 pkt 1-6 UODO);
 - realizacji prawa osoby do wniesienia sprzeciwu ze względu na jej szczególną sytuację (Art. 32 ust.1 pkt 7 UODO);
 - realizacji prawa osoby do wniesienia sprzeciwu wobec przetwarzania jej danych w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych (Art.32 ust. 1 pkt 8 UODO);
 - informowania osoby na jej wniosek osoby o przysługujących jej prawach w zakresie informacji, o których mowa w art. 32 ust. 1 pkt 1-5a. (Art. 33 UODO).
- c) sprawdzenie, czy pozyskiwane/przetwarzane dane są:
 - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (Art. 26 ust. 1 i 2 UODO);
 - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (Art. 26 ust. 1 pkt 3 UODO);
 - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (Art. 26 ust. 1 pkt 4 UODO).
- d) sprawdzenie umowy powierzenia pod kątem jej zawarcia na piśmie, wskazania zakresu i celu przetwarzania oraz obowiązku zabezpieczenia danych przez podmiot, któremu powierzono dane przed rozpoczęciem przetwarzania poprzez środki zabezpieczające zbiór danych, o których mowa w art. 36-39 (Art. 31 UODO);
- e) sprawdzenie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (Art. 36 ust. 1 UODO);
- f) sprawdzenie sposobu prowadzenia i zakresu dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w Art. 36 ust. 1 (Art. 36 ust. 2 UODO);
- g) sprawdzenie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
- h) sprawdzenie, czy osoby, które zostały upoważnione do przetwarzania danych, zobowiązane są zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (Art. 39 ust. 2 UODO);
- i) sprawdzenie, czy do przetwarzania danych są dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych (Art. 37

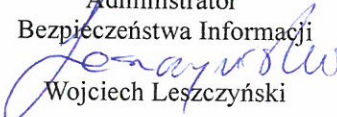
- UODO);
- j) sprawdzenie, czy Administrator danych zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (Art.38 UODO);
 - k) sprawdzenie, czy Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania (Art.39 ust. 1 UODO);
 - l) sprawdzenie wykonania obowiązku zgłoszenia / rejestracji zbiorów (Art. 40 UODO);
 - m) sprawdzenie przesłanek legalizujących przekazanie danych osobowych do państwa trzeciego (Art. 47 ust. 1 UODO);
 - n) sprawdzenie systemów informatycznych w zakresie spełnienia wymogów określonych w §7 ust. 1 oraz §7 ust. 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024);
 - o) Sprawdzenie stosowania środków bezpieczeństwa zawartych w Załączniku rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024):
 - zabezpieczeń fizycznych obszarów przetwarzana;
 - kontroli dostępu do danych w systemie informatycznym (uwierzytelnianie i rozliczalność);
 - zasad nadawania uprawnień w systemie informatycznym;
 - standardu bezpiecznych haseł;
 - wykonywania i zabezpieczenia kopii zapasowych zbiorów;
 - zabezpieczeń komputerów przenośnych poza obszarami przetwarzania;
 - zabezpieczeń nośników przeznaczonych do likwidacji, przekazania, naprawy;
 - monitoringu wdrożonych zabezpieczeń systemu informatycznego;
 - zapewnienia poufności i integralności danych na urządzeniach i nośnikach poza obszarami przetwarzania;
 - zabezpieczeń przeciw szkodliwemu oprogramowaniu;
 - zabezpieczeń przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
 - fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem (kontrola przepływu z siecią publiczną);
 - kryptografii teletransmisji w sieci publicznej (SSL / VPN).

III. PODSUMOWANIE

Po zakończeniu sprawdzenia ABI sporządza sprawozdanie z planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych za rok 2017 w terminie do 31 stycznia 2018 roku, które przekazuje administratorowi danych osobowych.

WÓJT

Magdalena Kołodziejczak

OPRACOWAŁ:
Administrator
Bezpieczeństwa Informacji

Wojciech Leszczyński