Warszawa, dnia 29 maja 2015 r.

Poz. 745

# ROZPORZĄDZENIE
# MINISTRA ADMINISTRACJI I CYFRYZACJI[1)]

z dnia 11 maja 2015 r.

**w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji**

Na podstawie art. 36a ust. 9 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) zarządza się, co następuje:

## Rozdział 1

## Przepisy ogólne

**§ 1.** Rozporządzenie określa tryb i sposób:

1) sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania w tym zakresie;

2) nadzorowania:

   a) opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,

   b) przestrzegania zasad określonych w dokumentacji, o której mowa w lit. a.

**§ 2.** Ilekroć w rozporządzeniu jest mowa o:

1) ustawie – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;

2) dokumentacji przetwarzania danych – należy przez to rozumieć dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, określoną w przepisach wydanych na podstawie art. 39a ustawy;

3) sprawdzeniu – należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

4) sprawozdaniu – należy przez to rozumieć dokument, o którym mowa w art. 36c ustawy, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia.

---

[1)] Minister Administracji i Cyfryzacji kieruje działem administracji rządowej – administracja publiczna, na podstawie § 1 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji (Dz. U. poz. 1254).

Rozdział 2

**Tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania**

**§ 3.** 1. Sprawdzenie jest dokonywane:

1) dla administratora danych;

2) dla Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem", w przypadku, o którym mowa w art. 19b ust. 1 ustawy.

2. Sprawdzenie jest przeprowadzane w trybie:

1) sprawdzenia planowego – według planu sprawdzeń, o którym mowa w ust. 3;

2) sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;

3) art. 19b ust. 1 ustawy – w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora.

3. Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.

4. Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:

1) z zasadami, o których mowa w art. 23–27 i art. 31–35 ustawy;

2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 ustawy oraz przepisach wydanych na podstawie art. 39a ustawy;

3) z zasadami przekazywania danych osobowych, o których mowa w art. 47–48 ustawy;

4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.

5. Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

6. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat.

7. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez administratora bezpieczeństwa informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

8. Administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia w trybie, o którym mowa w art. 19b ust. 1 ustawy, przed podjęciem pierwszej czynności w toku sprawdzenia.

**§ 4.** 1. Administrator bezpieczeństwa informacji dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

2. Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:

1) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

2) odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;

3) sporządzeniu kopii otrzymanego dokumentu;

4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;

5) sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

3. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności administratora bezpieczeństwa informacji mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności osoby zarządzającej tym systemem.

4. Materiały są sporządzane w postaci papierowej lub w postaci elektronicznej.

**§ 5.** 1. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia administratorowi bezpieczeństwa informacji przeprowadzenie czynności w toku sprawdzenia.

2. Administrator bezpieczeństwa informacji zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

3. Zawiadomienia nie przekazuje się w przypadku:

1) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;

2) sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin;

3) jeżeli kierownik jednostki organizacyjnej objętej sprawdzeniem posiada informacje, o których mowa w ust. 2.

**§ 6.** 1. Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje sprawozdanie.

2. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

3. Administrator bezpieczeństwa informacji przekazuje administratorowi danych sprawozdanie:

1) ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;

2) ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia;

3) ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – zachowując termin wskazany przez Generalnego Inspektora zgodnie z art. 19b ust. 1 ustawy.

Rozdział 3

**Tryb i sposób nadzoru nad dokumentacją przetwarzania danych**

**§ 7.** 1. Sprawując nadzór, o którym mowa w § 1 pkt 2, administrator bezpieczeństwa informacji dokonuje weryfikacji:

1) opracowania i kompletności dokumentacji przetwarzania danych;

2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;

3) stanu faktycznego w zakresie przetwarzania danych osobowych;

4) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;

5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

2. Administrator bezpieczeństwa informacji przeprowadza weryfikację:

1) w sprawdzeniach, o których mowa w § 3;

2) poza sprawdzeniami, na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych oraz własnego udziału administratora bezpieczeństwa informacji w procedurach w niej określonych.

3. Administrator bezpieczeństwa informacji może przeprowadzić weryfikację poza sprawdzeniami, na podstawie zgłoszenia osoby trzeciej.

**§ 8.** 1. W przypadku wykrycia podczas weryfikacji nieprawidłowości administrator bezpieczeństwa informacji:

1) zawiadamia administratora danych o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności;

2) zawiadamia administratora danych o nieaktualności dokumentacji przetwarzania danych oraz może przedstawić administratorowi danych do wdrożenia projekty dokumentów aktualizujących;

3) poucza lub instruuje osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres.

2. Zawiadomienia mogą być zawarte w sprawozdaniu albo w odrębnym dokumencie.

3. Pouczenia lub instrukcje są zawarte w odrębnym dokumencie skierowanym do osoby nieprzestrzegającej zasad określonych w dokumentacji przetwarzania danych.

4. Dokumenty, o których mowa w ust. 2 i 3, są sporządzane w postaci papierowej albo postaci elektronicznej.

Rozdział 4

**Przepis końcowy**

**§ 9.** Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Administracji i Cyfryzacji: *A. Halicki*