Projekt, 18.12.2014

R O Z P O R Z Ą D Z E N I E

M I N I S T R A A D M I N I S T R A C J I I C Y F R Y Z A C J I [1)]

z dnia ……2014 r.

w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych

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

[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. Nr 1254).

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, w szczególności w wyniku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem”;

4) sprawozdaniu – należy przez to rozumieć dokument zawierający elementy określone w art. 36c ustawy, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia, którego celem jest zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

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 w przypadku, o którym mowa w art. 19b ust. 1 ustawy.

2. Sprawdzenie dla administratora danych ma charakter:

1) sprawdzenia planowego – według planu sprawdzeń przygotowanego przez administratora bezpieczeństwa informacji, o którym mowa w ust. 3;

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

3. Plan sprawdzeń określa przedmiot poszczególnych sprawdzeń, zakres czynności, które będą podjęte w toku sprawdzenia oraz termin przeprowadzenia sprawdzenia.

4. Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności, potrzebę inwentaryzacji zbiorów danych osobowych przetwarzanych przez administratora danych 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 oraz art. 37-39 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 określony przez niego okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan jest przedstawiany administratorowi danych nie później niż na miesiąc przed rozpoczęciem okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

6. Sprawdzenie pozaplanowe jest przeprowadzane niezwłocznie po powzięciu przez administratora bezpieczeństwa informacji, informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia. Administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia pozaplanowego przed podjęciem pierwszej czynności w toku sprawdzenia.

7. Administrator danych przyjmuje od administratora bezpieczeństwa informacji do wiadomości plan sprawdzeń, a w przypadku sprawdzenia pozaplanowego, zawiadomienie o takim sprawdzeniu.

§ 4.1. Administrator bezpieczeństwa informacji określa:
1) zakres czynności, które będą podejmowane w toku sprawdzenia,
2) sposób i zakres dokumentowania czynności, o których mowa w pkt 1,
- niezbędnych do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

2. Przed każdym sprawdzeniem, administrator bezpieczeństwa informacji sporządza program sprawdzenia, który określa zakres czynności oraz sposób i zakres ich dokumentowania, zgodnie z ust. 1.

3. W toku sprawdzenia, administrator bezpieczeństwa informacji może podejmować następujące czynności:
1) zbieranie ustnych lub pisemnych wyjaśnień od osób objętych sprawdzeniem;
2) przeprowadzanie oględzin miejsc przetwarzania danych osobowych, a także uzyskiwanie dostępu do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
3) analizowanie dokumentów dotyczących przetwarzania danych osobowych.

4. Administrator bezpieczeństwa informacji może dokumentować czynności, o których mowa w ust. 3, poprzez utrwalenie danych z systemu informatycznego służącego do przetwarzania danych osobowych na informatycznym nośniku danych lub dokonanie wydruku tych danych, oraz poprzez sporządzenie:

1) notatki z czynności;
2) protokołu odebrania ustnych wyjaśnień;
3) protokołu z oględzin;
4) kopii otrzymanego dokumentu;
5) kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania danych osobowych;
6) kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

5. Notatkę z czynności podpisuje administrator bezpieczeństwa informacji. Protokół podpisuje administrator bezpieczeństwa informacji oraz każda osoba uczestnicząca w czynności. W przypadku odmowy podpisania protokołu przez osobę uczestniczącą w czynności, administrator bezpieczeństwa informacji sporządza w protokole stosowną adnotację.

6. W systemie informatycznym służącym do przetwarzania danych osobowych czynności, o których mowa w ust. 3, wykonywane są przy udziale osób upoważnionych do przetwarzania danych, w szczególności administratora systemu.

7. Dokumenty, o których mowa w ust. 4, sporządzane są w postaci papierowej albo w postaci elektronicznej.

8. Administrator bezpieczeństwa informacji, po uzgodnieniu z administratorem danych, może wystąpić o wydanie opinii przez osobę posiadającą wiedzę specjalistyczną nie dotyczącą przepisów o ochronie danych osobowych, niezbędną do zapewnienia prawidłowości przeprowadzanego sprawdzenia.

§ 5. 1. Osoba objęta sprawdzeniem bierze udział w czynności lub umożliwia administratorowi bezpieczeństwa informacji przeprowadzenie czynności, o których mowa w § 4 ust. 3.

2. Administrator bezpieczeństwa informacji zawiadamia osobę objętą sprawdzeniem o zakresie czynności z jej udziałem w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

3. Obowiązku zawiadomienia, o którym mowa w ust. 2, nie stosuje się w przypadku:

1) sprawdzenia pozaplanowego, jeżeli niezwłoczny udział osoby w czynnościach jest niezbędny 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.

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

2. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej. Sprawozdanie w postaci elektronicznej należy opatrzyć bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, lub, wyłącznie w przypadku sprawozdania dla Generalnego Inspektora, podpisem potwierdzonym profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r . poz. 1114).

3. Administrator bezpieczeństwa informacji przekazuje administratorowi danych sprawozdanie:
1) ze sprawdzenia planowego – w terminie określonym w planie sprawdzeń, nie później niż w terminie 30 dni od zakończenia sprawdzenia;
2) ze sprawdzenia pozaplanowego – niezwłoczne po zakończeniu sprawdzenia;
3) ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – w terminie umożliwiającym zachowanie przez administratora danych terminu wskazanego przez Generalnego Inspektora zgodnie z art. 19b ustawy.

§ 7. Sprawozdanie oraz dokumenty, o których mowa w § 4 ust. 4, administrator bezpieczeństwa informacji przechowuje przez okres co najmniej pięciu lat od dnia ich sporządzenia.

Rozdział 3

Tryb i sposób nadzoru nad dokumentacją przetwarzania danych

§ 8. Nadzór, o którym mowa w § 1 pkt 2, polega na 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) skuteczności przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych zabezpieczenia rozwiązań dla przeciwdziałania zagrożeniom dla ochrony danych osobowych;
5) przestrzegania obowiązków określonych w dokumentacji przetwarzania danych.

§ 9. 1. Weryfikacja, o której mowa w § 8, jest przeprowadzana przez administratora bezpieczeństwa informacji:
1) w sprawdzeniach, o których mowa w § 3;
2) poza sprawdzeniami, na podstawie zgłoszeń od osób wykonujących obowiązki określone w dokumentacji przetwarzania danych oraz własnego udziału administratora bezpieczeństwa informacji w procedurach w niej określonych.

2. Podczas weryfikacji administrator bezpieczeństwa informacji może wykonywać czynności, o których mowa w § 4 ust. 3.

§ 10. 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 przedstawia mu do wdrożenia dokumenty usuwające stan niezgodności;
2) zawiadamia administratora danych o nieaktualności dokumentacji przetwarzania danych oraz przedstawia administratorowi danych do wdrożenia dokumenty aktualizujące;
3) poucza lub instruuje osoby nieprzestrzegające zasad określonych w dokumentacji przetwarzania danych osobowych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, wskazując osoby odpowiedzialne za naruszenie tych zasad oraz jego zakres.

2. Zawiadomienia i pouczenia, o których mowa w ust. 1, mogą być zawarte w sprawozdaniu albo w odrębnym dokumencie sporządzonym w postaci papierowej albo postaci elektronicznej.

Rozdział 4

Przepisy przejściowe i końcowe

§ 11. Pierwszy plan sprawdzeń, o którym mowa w § 3 ust. 2 pkt 1, administrator bezpieczeństwa informacji przedstawia administratorowi danych w terminie 30 dni od dnia jego powołania, a w przypadku administratora bezpieczeństwa informacji, o którym mowa w art. 35 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. poz. 1662) – w terminie do dnia 30 kwietnia 2015 r.

§ 12. Wymagania dotyczące sprawdzeń oraz nadzoru nad dokumentacją przetwarzania danych określone w rozporządzeniu uważa się za spełnione, jeżeli administrator danych wdrożył system zarządzania bezpieczeństwem informacji z uwzględnieniem Polskiej Normy PN-ISO/IEC 27001, pod warunkiem, ze system ten obejmuje ochronę danych osobowych, a osobą wykonującą czynności w nim określone jest administrator bezpieczeństwa informacji.

§ 13. W przypadku administratorów danych będących podmiotami publicznymi w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, którzy wprowadzili audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 tej ustawy, sprawdzenie oraz nadzór na dokumentacją przetwarzania danych, mogą być wykonywane w ramach tego audytu, pod warunkiem, że wykonującym jest administrator bezpieczeństwa informacji.

§ 14. Administrator bezpieczeństwa informacji może upoważnić swoich zastępców, o których mowa w art. 36a ust. 6 ustawy, do wykonywania czynności lub opracowania dokumentów określonych w rozporządzeniu.

§ 15. Do administratora danych, o którym mowa w art. 36b ustawy, stosuje się odpowiednio przepisy rozporządzenia, z wyłączeniem obowiązków sporządzenia sprawozdania oraz zawiadomień, o których mowa w § 10 ust. 1. Administrator danych nie będący osobą fizyczną wskazuje osoby wykonujące czynności lub opracowujące dokumenty określone w rozporządzeniu.

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

MINISTER ADMINISTRACJI

I CYFRYZACJI

Za zgodność pod względem prawnym, legislacyjnym i redakcyjnym
- Katarzyna Kobierska, Dyrektor Departamentu Prawnego MAC
/-podpisano bezpiecznym podpisem elektronicznym weryfikowanym
przy pomocy ważnego kwalifikowanego certyfikatu/