Stowarzyszenie Administratorów Bezpieczeństwa Informacji

Warszawa 12.03.2015 r.

Uwagi Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji z dnia 4.03.2015 r.

W opinii Stowarzyszenia ABI doprecyzowania w projekcie rozporządzenia wymaga jeszcze kilka **bardzo istotnych zapisów, które będą miały wpływ na wykonywanie zadań przez administratorów bezpieczeństwa informacji.** Wprowadzenie zmian poprawiających czytelność zapisów rozporządzenia ułatwi właściwe wykonywanie zadań przez ABI, przez co wyeliminuje ryzyko popełniania przez nich błędów wynikających z niewłaściwej interpretacji czy rozumienia przepisów rozporządzenia.

§ 3 ust. 2 pkt 2

Należy dokonać korekty redakcyjnej - po słowach: "przez administratora bezpieczeństwa informacji" dodać słowo: "informacji". Proponowany zmieniony zapis:

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

§ 3 ust. 3

Proponujemy przeniesienie do § 3 ust. 3 zapisów z § 4 ust. 1 dotyczących sposobu i zakresu dokumentowania sprawdzenia, niezbędnych do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania. Uważamy, że zapisy takie powinny znaleźć się w ust. 3, który opisuje co ma być określone w planie sprawdzenia. Zasady dokumentowania sprawdzeń ABI powinien określić właśnie w planie sprawdzenia. Zamieszczenie tych informacji w jednym miejscu ułatwi przygotowywanie planów ABI. Poza tym proponujemy zmianę zapisów dotyczących terminu, tak aby termin odnosił się do „sprawdzeń”, a nie „sprawdzenia”.

Proponowane nowe brzmienie zapisów § 3 ust. 3:

„3. Plan sprawdzeń określa przedmiot, zakres sprawdzenia, sposób i zakres dokumentowania sprawdzenia, niezbędny do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania, a także termin przeprowadzenia sprawdzeń.”

§ 3 ust. 4

Proponujemy niezbędną zmianę zapisów ust. 4 dla ich lepszej przejrzystości. Zapis w ust. 4 jest nieczytelny, nie bardzo wiadomo co oznacza sformułowanie „uwzględnia w szczególności zbiory danych osobowych i systemy informatyczne”. Sprawdzanie zbiorów danych przetwarzanych przez ADO oraz systemów informatycznych służących do przetwarzania danych jest przecież przedmiotem sprawdzenia. Proponujemy podział ust. 4 na ust. 4 i 5. W ust. 4 powinien zostać zdefiniowany przedmiot sprawdzenia, a w ust. 5 informacja jakie zasady ochrony danych powinny być uwzględnione przez ABI podczas przeprowadzanej weryfikacji zgodności przetwarzania danych z przepisami.

Proponowane nowe brzmienie zapisów § 3 ust. 4 i 5:

„4. Przedmiotem sprawdzenia są w szczególności zbiory danych osobowych, systemy informatyczne służące do przetwarzania danych osobowych oraz weryfikacja zgodności przetwarzania danych z obowiązkami określonymi w ustawie”.

„5. Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności 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.”

§ 3 ust. 5

Proponujemy wykreślenie ostatniego zdania w ust. 5., ponieważ plan, który nie zawiera przynajmniej jednego sprawdzenia nie istnieje. ABI zgodnie z obowiązkiem wynikającym z § 3 ust. 2 musi sporządzić plan sprawdzeń. Naszym zdaniem ABI w wykonywaniu swoich obowiązków, nie powinien być obarczony formalistycznymi "ilościowymi wskaźnikami".

Proponujemy również dodanie do tego ustępu zapisu dotyczącego terminu przedstawienia ADO pierwszego planu sprawdzeń przez ABI. Zapis ten był zawarty w § 11 poprzedniej wersji projektu rozporządzenia, który został w nowej wersji projektu wykreślony.

Proponowane nowe brzmienie zapisów § 3 ust. 5 (po zmianie numeracji zgodnie z poprzednią propozycją będzie to ust. 6):

„6. Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan jest przedstawiany administratorowi danych nie później niż na miesiąc przed dniem rozpoczęcia okresu objętego planem. Pierwszy plan sprawdzeń, administrator bezpieczeństwa informacji przedstawia administratorowi danych w terminie 30 dni od dnia jego powołania.”

§ 3 ust. 6

Nowy zapis, który został dodany już po konferencji uzgodnieniowej wprowadza zamieszanie interpretacyjne co do wymaganych terminów przeprowadzenia sprawdzeń. Umieszczenie tego przepisu w projekcie rozporządzenia jest niepotrzebnym wprowadzaniem "ilościowych wskaźników" wykonywania obowiązków ABI. Z przepisów § 3 ust. 1, 2 i 3 niezbicie wynika obowiązek przeprowadzania sprawdzeń i objęcia nimi wszystkich zbiorów i systemów informatycznych. ABI, znając wymogi i zagrożenia przetwarzania danych w zbiorach i systemach u niego funkcjonujących, powinien kompetentnie decydować o kolejności i częstotliwości dokonywania ich sprawdzeń i ponosić za to odpowiedzialność. Dowodem objęcia sprawdzeniami wszystkich zbiorów i systemów będzie zestawienie inwentarza zbiorów oraz przedmiotu i zakresu wykonanych i planowanych sprawdzeń.

Proponujemy wykreślenie ust. 6 wprowadzającego formalny obowiązek objęcia sprawdzeniem każdego zbioru danych i systemu informatycznego co 2 lata.

Natomiast jeżeli zapis ten miałby pozostać to należy rozszerzyć termin z 2 na 5 lat. Argumentujemy to sytuacją dużych podmiotów, pracujących w oparciu o zaawansowane systemy informatyczne, gdzie częste przeprowadzanie takiego sprawdzenia może być znacznie utrudnione. Z drugiej strony w takich podmiotach aplikacji służących do przetwarzania danych osobowych może być ponad 100 lub znacznie więcej. Poza tym są ADO, którzy w swoich wykazach zbiorów danych osobowych posiadają ponad 100 zbiorów danych osobowych. W przypadku takich podmiotów przeprowadzanie sprawdzenia w trybie 2 letnim wszystkich systemów i zbiorów, odbywałoby się w trybie ciągłym. Dlatego istnieje uzasadniona potrzeba rozszerzenia czasu do 5 lat, w przypadku wprowadzania takich wymagań.

Odrębną sprawą do doprecyzowania jest wprowadzenie w ust. 6 wymogu objęcia sprawdzaniem oprócz systemów informatycznych służących do przetwarzania również systemów zabezpieczania danych osobowych. Sprawdzenie takie ma odnosić się do przepisów wykonawczych przyjętych na podstawie art. 39a ustawy o ochronie danych osobowych. Rozporządzenie MSWiA 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) nie definiuje systemów zabezpieczania danych osobowych, jest mowa w nim o systemie informatycznym, dla którego zdefiniowane są poziomy bezpieczeństwa oraz opis środków bezpieczeństwa, który ma być stosowany na poszczególnych poziomach. Dlatego należy usunąć zapisy o systemach zabezpieczania danych osobowych jako niezgodne z wymaganiami ustawowymi.

W sytuacji pozostawienia jednak ust. 6 proponujemy jego nowe brzmienie (po zmianie numeracji zgodnie z poprzednimi propozycjami będzie to ust. 7):

„7. Każdy zbiór danych oraz system informatyczny służący do przetwarzania danych osobowych powinien być objęty sprawdzeniem co najmniej raz na pięć lat."

§ 3 ust. 8

Proponujemy w §3 zmienić treść ust. 8 i objąć zakresem powiadomienia ADO również sprawdzenie wynikające z wystąpienia GIODO w trybie art. 19b ustawy. W naszej ocenie bardzo niekomfortową byłaby sytuacja prowadzenia sprawdzenia przez ABI w trybie 19b, bez wiedzy ADO, podczas, gdy w przypadku kontroli przeprowadzanej przez GIODO ADO otrzymuje taką informację.

Proponowane nowe brzmienie zapisów § 3 ust. 8 (po zmianie numeracji zgodnie z poprzednimi propozycjami będzie to ust. 9):

„9. Administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia, o którym mowa w ust. 2 pkt 2 i 3 przed podjęciem pierwszej czynności w toku sprawdzenia."

§ 4 ust. 1

Proponujemy wykreślenie tego ustępu i przeniesienie jego zapisów do § 3 ust. 3 (zgodnie z komentarzem powyżej).

§ 4 ust. 2

Ust. 2 należy zamienić na ust. 1, doprecyzować i przeredagować tak aby zapisy były czytelne.

W stosunku do poprzedniej wersji projektu rozporządzenia z 18.12.2014 r. nastąpiła zmiana w obowiązkach dokumentowania czynności sprawdzenia. W poprzedniej wersji § 4 ust. 4 znajdował się zapis: „ *Administrator bezpieczeństwa informacji **może** dokumentować czynności, o których mowa w ust. 3, poprzez….."*. W nowej wersji w ust. 2 znajdują się zapisy: *„Administrator bezpieczeństwa informacji dokumentuje przeprowadzenie czynności w szczególności poprzez…."*. Zostało wykreślone słowo ***„może",*** które było istotne z punktu widzenia możliwości wyboru sposobu dokumentowania czynności sprawdzenia przez ABI – a takie były intencje przy tworzeniu tych zapisów. Nowa forma zapisów sugeruje obowiązek wykonywania wszystkich czynności wymienionych w ust. 2 przez ABI, co powoduje że ABI staje się właściwie inspektorem GIODO.

Należy zatem przywrócić zapis o możliwości wyboru sposobu dokumentowania sprawdzenia przez ABI.

Proponujemy wymienienie wszystkich możliwych czynności dokumentowania w kolejnych punktach. Proponujemy również zamianę sformułowania „utrwalenie danych z systemu informatycznego" na „utrwalenie informacji z systemu informatycznego", ponieważ słowo dane może kojarzyć się z

utrwalaniem danych osobowych, a nie chodzi tu o to aby ABI kopiował dane z systemu informatycznego, może natomiast zaistnieć potrzeba skopiowania z systemu pewnych informacji, dotyczących przetwarzania danych.

Proponowane nowe brzmienie zapisów § 4 ust. 2 (po zmianie numeracji zgodnie z poprzednimi propozycjami będzie to ust. 1):

„4. 1. Administrator bezpieczeństwa informacji może dokumentować przeprowadzenie czynności wykonywanych w trakcie sprawdzenia w szczególności poprzez:

1) utrwalenie informacji z systemu informatycznego służącego do przetwarzania danych osobowych na informatycznym nośniku danych;

2) dokonanie wydruku tych danych;

3) sporządzenie 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;

4) odebranie pisemnych wyjaśnień od osoby, której czynności objęto sprawdzeniem;

5) sporządzenie kopii otrzymanych dokumentów;

6) sporządzenie kopii obrazów wyświetlonych na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania danych osobowych;

7) sporządzenie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu."

§ 4 ust. 5

W związku ze zmianą zapisów w § 4 ust. 2, należy dodać właściwe odniesienie § 4 ust. 1. Proponujemy również doprecyzować słowo „materiały" sformułowaniem „dokumentacyjne".

Proponowane nowe brzmienie zapisów § 4 ust. 5 (po zmianie numeracji zgodnie z poprzednimi propozycjami będzie to ust. 4):

4. Materiały dokumentacyjne, o których mowa w ust. 1, sporządzane są w postaci papierowej lub w postaci elektronicznej.