JULIA KAMIŃSKA-KASJANIUK

Metodyka pracy administratora bezpieczeństwa informacji

JDS CONSULTING

Julia Kamińska-Kasjaniuk

Metodyka pracy administratora bezpieczeństwa informacji

Wydanie 1

Warszawa 2016

Stan prawny: czerwiec 2016
Autor: Julia Kamińska-Kasjaniuk
Wydawca: JDS Consulting sp. z o.o. sp.k.

ISBN **978-83-65364-01-2**
Wydanie 1

Skład wersji elektronicznej

konwersja.virtualo.pl

Spis treści

Wykaz skrótów

Od autora

1. Zadania administratora bezpieczeństwa informacji

2. Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych

    a. Prowadzenie sprawdzeń planowych

    b. Prowadzenie sprawdzeń doraźnych

    c. Prowadzenie sprawdzeń na żądanie Generalnego Inspektora Ochrony Danych Osobowych

3. Nadzór nad dokumentacją przetwarzania danych

4. Prowadzenie rejestru zbiorów danych

5. Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

6. Rola administratora bezpieczeństwa informacji w przypadkach wystąpienia incydentów związanych z bezpieczeństwem przetwarzanych danych osobowych

7. Postępowanie administratora bezpieczeństwa informacji w sytuacji otrzymania zapytania lub skargi od podmiotu danych

8. Kontrola Generalnego Inspektora Ochrony Danych Osobowych

9. Rejestracja zbiorów danych osobowych w rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych

10. Wzory dokumentów

11. Akty prawne

Bibliografia

O autorce

Przypisy

Wszystkie rozdziały dostępne w pełnej wersji książki.

Wykaz skrótów

ustawa o ochronie danych osobowych – ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.)

RozpDok – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. Nr 100, poz. 1024)

RozpABI – rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r. poz. 745)

RozpRejestr - rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. z 2015 r. poz. 719)

kpa – ustawa z dnia 14 czerwca 1960 roku Kodeks postępowania administracyjnego (t.j. Dz. U. z 2016 r. poz. 23 ze zm.)

GIODO – Generalny Inspektor Ochrony Danych Osobowych

SN – Sąd Najwyższy

NSA – Naczelny Sąd Administracyjny

WSA – Wojewódzki Sąd Administracyjny

Dz. U. – Dziennik Ustaw

art. – artykuł

ust. – ustęp

pkt - punkt

t.j. – tekst jednolity

poz. - pozycja

wyr. - wyrok

r. - rok

Od autora

Niniejsza publikacja powstała z myślą o tych, którzy rozpoczynają swoją pracę w zawodzie administratora bezpieczeństwa informacji lub pełniąc tę funkcję od lat, chcą zapoznać się doświadczeniem i poglądami innych. Publikacja ma charakter praktycznego komentarza zawierającego wskazówki dotyczące wykonywania zadań administratora bezpieczeństwa informacji. Jako radca prawny skupiam się na prawnych aspektach pełnienia tej funkcji, uzupełniając je przykładami z praktyki pracy w wielu podmiotach i organizacjach. Ponadto część rozdziałów zawiera fragmenty orzeczeń i decyzji, mających istotne znaczenie dla wykonywania obowiązków.

Jestem administratorem bezpieczeństwa informacji od 2003 roku. Gdy zaczynałam pracę na tym stanowisku nikt właściwie nie myślał, że będzie to w przyszłości zawód. Choć i obecnie zdarza się, iż zadania administratora bezpieczeństwa informacji zostają zlecone do wykonywania „dodatkowo" do piastowania innego stanowiska. Myślę, iż wynika to przede wszystkim z niewiedzy pracodawców o tym jak istotne, trudne i odpowiedzialne zadanie powierzają.

Życzę obecnym administratorom bezpieczeństwa informacji czy przyszłym inspektorom ochrony danych aby praca na tym stanowisku dawała im wiele satysfakcji, a także by byli i czuli się doceniani.

Zadania administratora bezpieczeństwa informacji

Od stycznia 2015 roku w wyniku nowelizacji[1] ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych[2] został doprecyzowany zakres obowiązków administratora bezpieczeństwa informacji.

W miejsce dotychczas obowiązującego ogólnego zapisu, iż administrator bezpieczeństwa informacji nadzoruje przestrzeganie zasad ochrony aktualnie, wskazano na zadania, jakie realizować ma administrator bezpieczeństwa informacji.

Zadania te podzielone zostały na dwie grupy:

− zapewnienie przestrzegania przepisów o ochronie danych osobowych,

− prowadzenie rejestru zbiorów danych.

Zgodnie z art. 36a ust. 1 pkt 1 ustawy o ochronie danych osobowych do administratora bezpieczeństwa informacji należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

− sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

− nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych,

− zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Warto zwrócić uwagę na redakcję art. 36a ust. 1 pkt 1, który mówi o tym, że zapewnianie przestrzegania przepisów ma być realizowane w „szczególności przez", co oznacza, iż katalog zadań, jakie powinien podejmować administrator bezpieczeństwa informacji nie jest zamknięty i ograniczony do wymienionych obowiązków. Dla administratora bezpieczeństwa informacji ważne jest osiągnięcie postawionego w tym przepisie celu jakim jest zapewnianie przestrzegania przepisów. A zatem przykładowo wśród innych niż wymienione zadań, które będą prowadziły do realizacji tego celu, można wymienić m.in.:

− opiniowanie w sprawie możliwości oraz prawidłowości zbierania danych osobowych,

− przygotowanie wniosków rejestracyjnych zbiorów danych do rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych,

− reprezentacja administratora danych w postępowaniu rejestracyjnym przed GIODO,

− udzielanie osobom, których dane osobowe są przetwarzane, odpowiedzi na złożoną skargę lub zapytanie,

− przygotowywanie oraz opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych,

− opiniowanie w przedmiocie udostępniania danych,

− reprezentacja administratora danych w postępowaniu kontrolnym prowadzonym przez GIODO.

Zwraca uwagę jeszcze jedno sformułowanie, tj. „zapewnianie". Oznacza to, iż praca administratora bezpieczeństwa informacji w tym zakresie ma charakter ciągły.

W przypadkach obu rodzajów zadań wymienionych w ustawie, doszczegółowienie sposobów ich realizacji znajdziemy w aktach wykonawczych, takich jak:

− rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r. poz. 745),

− rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. z 2015 r. poz. 719).

W ww. rozporządzeniach doprecyzowane zostały sposoby realizacji zadań, w tym nawet poszczególne rodzaje czynności, jakie powinny być wykonywane przez administratora bezpieczeństwa informacji.

Na marginesie warto odnotować, iż już za dwa lata, od 25 maja 2018 roku, administratora bezpieczeństwa informacji zastąpi inspektor ochrony danych w związku z uchwaleniem i publikacją Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[3]. Jak wynika z treści ogólnego rozporządzenia, choć rola i zadania administratora bezpieczeństwa informacji i inspektora ochrony danych są podobne, to jednak nie takie same i z pewnością konieczne stanie się odrębne omówienie obowiązków inspektora ochrony danych.

Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych

Sprecyzowanie obowiązków administratora bezpieczeństwa informacji w zakresie prowadzenia sprawdzania zgodności przetwarzania danych oraz opracowania sprawozdania zostało dokonane w rozporządzeniu Ministra Administracji i Cyfryzacji 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. W tym właśnie akcie zawarto legalną definicję sprawdzenia, które – zgodnie z nią – oznacza „czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych". RozpABI wymienia trzy tryby (przypadki), w których administrator bezpieczeństwa informacji prowadzi sprawdzenia:

− sprawdzenia planowe
− sprawdzenia doraźne
− sprawdzenia na żądanie Generalnego Inspektora Ochrony Danych Osobowych.

Prowadzenie sprawdzeń planowych

Sprawdzenie planowe to takie, które jest wykonywane na podstawie planu sprawdzeń, opracowywanego przez administratora bezpieczeństwa informacji. Sporządzenie planu poprzedza przeprowadzenie samego sprawdzenia i stanowi element przygotowania do jego przeprowadzenia. Plan sprawdzeń może obejmować jedno, jak i kilka sprawdzeń. Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.

Przedmiot sprawdzenia wskazuje na to jakie zagadnienia będą objęte sprawdzeniem i powinien uwzględniać zbadanie wykonywania obowiązków, spoczywających na administratorze danych, o których mowa w art. 23-27, 31, 31a, 33, 35-39a, 40, 47-48 ustawy o ochronie danych osobowych. Ponadto przedmiot odnosić powinien się do zbiorów danych osobowych, rodzajów danych osobowych oraz form przetwarzania danych. Przykładowo jako przedmioty sprawdzeń można wskazać: prowadzenie ewidencji osób upoważnionych, realizację obowiązków informacyjnych wobec klientów, zabezpieczenie systemów informatycznych służących do przetwarzania danych osobowych, legalność przetwarzania danych kandydatów do pracy.

Zakres przedmiotu obejmować powinien doprecyzowanie przedmiotu. W przypadku zawężenia przedmiotu sprawdzenia zakres sprawdzenia to poszczególne czynności, które będą podejmowane w ramach prowadzenia sprawdzenia. Przykładowo dla przedmiotu – ewidencja osób upoważnionych do przetwarzania danych osobowych zakres obejmie m.in.:

− sprawdzenie faktu prowadzenia ewidencji osób upoważnionych przez osobę zobowiązaną zgodnie z polityką bezpieczeństwa,
− zbadanie zgodności zakresu ewidencji z wymaganiami ustawy o ochronie danych osobowych oraz obowiązującym wzorem zawartym w polityce bezpieczeństwa,
− porównanie zapisów ewidencji z wydanymi upoważnieniami do przetwarzania danych osobowych,

− porównanie zapisów ewidencji z rejestrem uprawnień w systemach informatycznych,
− badanie aktualności ewidencji osób upoważnionych.

Z kolei im szersze określenie przedmiotu sprawdzenia, tym bardziej ogólne określenie jego zakresu poprzez odwołanie do ustawowych obowiązków. Przykładowo w odniesieniu do sprawdzenia prawidłowości przetwarzania danych w zbiorze kadrowo-płacowym zakres obejmować może:
− legalność przetwarzania danych osobowych pracowników,
− poprawność i adekwatność przetwarzania danych osobowych,
− spełnienie obowiązków informacyjnych względem pracowników i formy spełnienia tych obowiązków,
− zabezpieczenie danych osobowych przetwarzanych w formie papierowej,
− zabezpieczenia systemu informatycznego, w którym przetwarzane są dane kadrowo-płacowe, z uwzględnieniem wymogów dla aplikacji, w których przetwarzane są dane osobowe,
− nadanie upoważnień do przetwarzania danych osobowych osobom posiadającym dostęp do zbioru kadrowo-płacowego,
− zakres i cel udostępnienia danych ze zbioru, legalność udostępniania danych oraz odnotowywanie udostępnień,
− badanie zgodności przetwarzania danych w odniesieniu do zbioru kadrowo-płacowego z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

W ust. 6 § 3 RozpABI postawiony został wymóg aby zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych zostały objęte sprawdzeniem co najmniej raz na pięć lat. Powyższe oznacza konieczność dokonywania w cyklach pięcioletnich sprawdzenia kompleksowego obejmującego wszystkie zasoby oraz zastosowane zabezpieczenia.

W odniesieniu do terminu prowadzenia sprawdzenia ujętego w planie sprawdzeń określono, iż termin ten musi mieścić się w ramach czasowych wyznaczonych przez treść RozpABI, które stanowi, iż:
− plan sprawdzenia sporządzany na okres nie krótszy niż kwartał i nie dłuższy niż rok (przy czym konkretne terminy, w jakich będzie wykonywane sprawdzenie czy sprawdzenia ujęte w planie sprawdzeń określa administrator bezpieczeństwa informacji, mając na uwadze okres obowiązywania samego planu),
− plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem (a zatem sprawdzenie planowe nie powinno rozpocząć się wcześniej niż po upływie 2 tygodni od przedstawienia planu),
− plan sprawdzeń obejmuje co najmniej jedno sprawdzenie (co oznacza konieczność przeprowadzenia minimum jednego sprawdzenia w roku).

Plan sprawdzenia określa również sposób i zakres dokumentowania sprawdzeń, co należy odnieść do oczekiwanych na gruncie rozporządzenia form dokumentowania czynności podejmowanych w ramach prowadzonych sprawdzeń. A zatem dla zakresu dokumentowania będą to przykładowo:
1. odebranie ustnych wyjaśnień od pracowników co do sposobu wykonywania postanowień polityki bezpieczeństwa, dotyczących prowadzenia ewidencji osób upoważnionych,
2. wgląd do treści ewidencji osób upoważnionych,

3. wgląd do wydanych upoważnień,
4. odebranie wyjaśnień dotyczących aktualnego stanu zatrudnienia.

I adekwatnie do powyższego – w odniesieniu do sposobu dokumentowania:
1. protokół odebrania ustnych wyjaśnień (dla czynności wymienionych w pkt 1 i 4 zakresu dokumentowania czynności),
2. notatka z czynności (dla czynności wskazanych w pkt 2 i 3 zakresu dokumentowania czynności).

Plan sprawdzenia powinien zostać przedstawiony przez administratora bezpieczeństwa informacji administratorowi danych minimum na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Przepisy prawa nie wskazują aby administrator danych miał akceptować przedłożony plan czy też w jakikolwiek sposób się do niego ustosunkowywać. Przedstawienie jest czynnością o charakterze informacyjnym. Brak w przepisach ustalonej formy planu sprawdzenia. Oznacza to, że może zostać on przygotowany w dowolnej formie, w tym ustnie. Dla celów dowodowych, jak również ze względów praktycznych plany sprawdzeń są przygotowywane zwykle w postaci elektronicznej albo papierowej.

Sprawdzenie prowadzone jest na podstawie i w granicach określonych w planie. Przed podjęciem zaplanowanych czynności sprawdzenia administrator bezpieczeństwa informacji zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności (§ 5 ust. 2 RozpABI). W przepisie tym mowa o kierowniku działu, departamentu lub zespołu, którego działalność oraz pracownicy mają być objęci sprawdzeniem. Administrator bezpieczeństwa informacji jest zobowiązany do dokumentowania czynności, które podejmuje w ramach prowadzonego sprawdzenia w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania. Jak wskazuje § 4 ust. 2 RozpABI, 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.

Wyliczenie sposobów dokumentowania czynności ma charakter jedynie przykładowy. Poza wymienionymi w tym przepisie możliwymi sposobami są również np.:
− przekazanie ankiety do wypełnienia,
− sporządzenie fotografii z miejsc zabezpieczenia danych,
− sporządzenie protokołu podpisywanego przez wszystkich obecnych z: oględzin, wyjaśnień, okazania,

− wywiad z osobą upoważnioną do przetwarzania danych.

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. Ponadto osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia administratorowi bezpieczeństwa informacji przeprowadzenie czynności w toku sprawdzenia.

Materiały z dokumentowania czynności mogą mieć postać papierową lub elektroniczną, co jest skorelowane z formą sprawozdania ze sprawdzenia, do którego będą stanowiły one załączniki.

Z przeprowadzonego sprawdzenia planowego administrator bezpieczeństwa informacji sporządza sprawozdanie.

Zgodnie z definicją legalną, sprawozdanie to dokument, o którym mowa w art. 36c ustawy o ochronie danych osobowych, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia. Elementy, z jakich powinno składać się sprawozdanie wymienione, zostały enumeratywnie w art. 36c ustawy o ochronie danych osobowych. Są to:

1. oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania,
2. imię i nazwisko administratora bezpieczeństwa informacji,
3. wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach,
4. data rozpoczęcia i zakończenia sprawdzenia,
5. określenie przedmiotu i zakresu sprawdzenia,
6. opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
7. stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem,
8. wyszczególnienie załączników stanowiących składową część sprawozdania,
9. podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania,
10. data i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.

Sprawozdanie musi zostać sporządzone w postaci elektronicznej albo papierowej. W przypadku postaci elektronicznej powinno zostać opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu. W praktyce administrator bezpieczeństwa informacji często sporządza dwa egzemplarze sprawozdania lub wykonuje jego kopię dla celów dowodowych i dokumentacyjnych. Sprawozdanie ze sprawdzenia planowego należy sporządzić i przekazać administratorowi danych nie później niż w terminie 30 dni od zakończenia sprawdzenia.

Prowadzenie sprawdzeń doraźnych

Sprawdzenie doraźne to sprawdzenie przeprowadzane przez administratora bezpieczeństwa informacji

w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez niego wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia. Szerzej na temat sytuacji kwalifikowanych jako naruszenie ochrony danych opisane zostało w Rozdziale 6 „Rola administratora bezpieczeństwa informacji w przypadkach wystąpienia incydentów związanych z bezpieczeństwem przetwarzanych danych osobowych".

W tym miejscu skoncentrujemy się na czynnościach, jakie powinien podjąć administrator bezpieczeństwa informacji w ramach wykonania czynności samego sprawdzenia doraźnego.