Wykonywanie sprawdzeń przez ABI – od planu do sprawozdania

Jarosław Żabówka

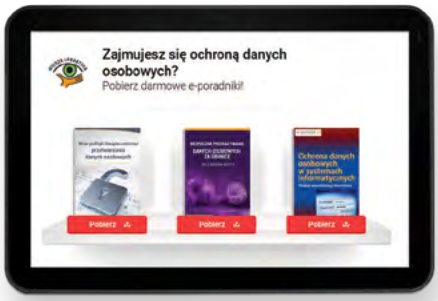
WIEDZA i PRAKTYKA

Ochrona i przetwarzanie danych osobowych

WYJĄTKOWE EBOOKI
ZA DARMO DLA CIEBIE

Jeśli:

- ✔ jesteś właścicielem firmy, zarządzasz urzędem albo placówką oświatową,
- ✔ gromadzisz dane swoich klientów lub pracowników,
- ✔ jesteś administratorem bezpieczeństwa informacji (ABI),
- ✔ chcesz być na bieżąco z najnowszymi przepisami dotyczącymi Ochrony danych osobowych,



WEJDŹ NA STRONĘ
www.pobierzebook.wip.pl/odo
i pobierz bezpłatne e-poradniki!

Pobierz

Nie przegap!

„Oficyna Prawa Polskiego”
Wydawnictwo WiP
ul. Łotewska 9A, 03–918 Warszawa

NIP: 526–19–92–256

KRS: 0000098264 – Sąd Rejonowy dla m.st. Warszawy,
Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy
Wysokość kapitału zakładowego: 200.000 zł

Redaktor: Wioleta Szczygielska

Kierownik grupy wydawniczej: Agnieszka Konopacka-Kuramochi

Wydawca: Weronika Wota

Koordynacja produkcji:
Mariusz Jezierski, Magdalena Huta

Korekta: Zespół

Projekt graficzny okładki: Michał Marczewski

Skład i łamanie: Ireneusz Gawliński

E-book „Wykonywanie sprawdzeń przez ABI – od planu do sprawozdania” jest chroniony prawem autorskim. Przedruk materiałów opublikowanych w e-booku – bez zgody wydawcy – jest zabroniony. Zakaz nie dotyczy cytowania publikacji z powołaniem się na źródło.
Publikacja została przygotowana z zachowaniem najwyższej staranności i wykorzystaniem wysokich kwalifikacji, wiedzy i doświadczenia autorów oraz konsultantów. Zaproponowane w publikacji wskazówki, porady i interpretacje nie mają charakteru porady prawnej. Ich zastosowanie w konkretnym przypadku może wymagać dodatkowych, pogłębionych konsultacji. Publikowane rozwiązania nie mogą być traktowane jako oficjalne stanowisko organów i urzędów państwowych. W związku z powyższym redakcja nie może ponosić odpowiedzialności prawnej za zastosowanie zawartych w publikacji wskazówek, przykładów, informacji itp. do konkretnych przypadków.

Informacje o prenumeracie:
tel.: 22 518 29 29 faks: 22 617 60 10
e-mail: cok@opp.com.pl

Jednym z obowiązków, jakie na administratora bezpieczeństwa informacji (ABI) nałożyła nowelizacja ustawy o ochronie danych osobowych z 1 stycznia 2015 r., jest konieczność zapewnienia przestrzegania przepisów o ochronie danych osobowych. ABI powinien realizować ten obowiązek m.in. poprzez sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator bezpieczeństwa informacji przeprowadza sprawdzenie w trzech sytuacjach – gdy wynika to z planu sprawdzeń (sprawdzenie planowe), gdy dojdzie do incydentu, który narusza bezpieczeństwo danych osobowych (sprawdzenie doraźne) i gdy o przeprowadzenie sprawdzenia zwróci się do ABI Generalny Inspektor Ochrony Danych Osobowych (GIODO). To ostatnie sprawdzenie przebiega tak, jak sprawdzenie planowe. Różni się od niego jedynie zakresem, gdyż ten jest wskazywany przez GIODO, a nie ustalany samodzielnie przez ABI.

Z każdego sprawdzenia administrator bezpieczeństwa informacji musi przygotować sprawozdanie. ABI przedstawia je administratorowi danych osobowych (ADO). Sprawozdanie ze sprawdzenia, które zostało przeprowadzone na zlecenie Generalnego Inspektora Ochrony Danych Osobowych, trafia za pośrednictwem administratora danych do GIODO.

Plan sprawdzeń

Plan sprawdzeń to prosty dokument, ma jednak podstawowe znaczenie dla realizacji zadań administratora bezpieczeństwa informacji. Błędy popełnione przy opracowywaniu planu mogą skutkować problemami, które pojawią się dopiero za kilka lat. Dlatego warto poświęcić czas na przemyślane opracowanie tego dokumentu, który jest jednym z podstawowych narzędzi pracy ABI. Jednym z zadań administratora bezpieczeństwa informacji jest „sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych" (art. 36a ust. 1 lit. a uodo). Sposób realizacji tego zadania określony został w rozporządzeniu ministra administracji i cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 29 maja 2015 r).

Rozporządzenie określa trzy tryby prowadzenia sprawdzenia przez administratora bezpieczeństwa informacji (ABI). Jednym z nich jest sprawdzenie planowe, prowadzone według opracowanego przez ABI planu sprawdzeń. Celem opracowania planu jest umożliwienie osobom i komórkom objętym sprawdzeniem odpowiedniego przygotowania, pozwalającego na sprawne przeprowadzenie sprawdzenia i minimalizację zakłóceń realizacji procesów biznesowych. Plan sprawdzeń służy również zapewnieniu, że sprawdzeniami objęte zostaną wszystkie zbiory danych i systemy informatyczne służące do przetwarzania danych.

Plan określa działania, które ABI podejmie podczas sprawdzeń. Jest on przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Jeśli ABI nie został powołany, nie mamy obowiązku opracowania planu sprawdzeń – rozporządzenie dotyczy jedynie trybu i sposobu realizacji zadań przez ABI. Jednak również gdy ABI nie zostanie

powołany, plan sprawdzeń może być przydatnym narzędziem, zapewniającym, że „sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych" będzie rzeczywiście realizowane.

Zawartość planu, określona w § 3 ust. 3 rozporządzenia, uwzględnia dla poszczególnych sprawdzeń: przedmiot, zakres, termin przeprowadzenia, sposób i zakres dokumentowania.
Zgodnie z § 3 ust. 4 rozporządzenia:

1. „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 z:

- zasadami, o których mowa w art. 23–27 i art. 31–35 ustawy,
- zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 ustawy oraz przepisach wydanych na podstawie art. 39a ustawy,
- zasadami przekazywania danych osobowych, o których mowa w art. 47–48 ustawy,
- obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy".

W praktyce oznacza to, że w kolejnych sprawdzeniach należy uwzględnić wszystkie aspekty przetwarzania danych, we wszystkich zbiorach i wszystkich systemach informatycznych. Decyzja, w jakiej kolejności sprawdzać te zagadnienia, pozostawiona została administratorowi bezpieczeństwa informacji. W zależności od zakresu przetwarzanych danych, sposobu ich przetwarzania, potrzeb organizacji i własnego doświadczenia, ABI musi zdecydować o zakresach kolejnych sprawdzeń. W planie sprawdzeń ABI powinien wskazać zbiory, systemy i zasady przetwarzania objęte konkretnym sprawdzeniem.

Określając przedmiot, zakres i terminy sprawdzeń, administrator bezpieczeństwa informacji musi wziąć pod uwagę szereg czynników:

- Złożoność i liczbę procesów realizowanych przez komórki oraz zakresy przetwarzanych danych osobowych.
- Konieczność częstszego prowadzenia sprawdzeń w komórkach, w których ryzyko niezgodnego z prawem przetwarzania danych jest większe (np. przetwarzane są dane wrażliwe, częściej zmieniane są procesy przetwarzania danych, występuje większa rotacja pracowników, wymieniane są systemy informatyczne itd.).
- Doświadczenie w prowadzeniu sprawdzeń i audytów.
- Możliwość niepowodzenia przeprowadzenia sprawdzenia i konieczność jego powtórzenia.

Planując termin sprawdzenia, ABI powinien uwzględnić:

- Dostępność osób i informacji – zaplanowanie sprawdzenia w okresie urlopowym lub w czasie zwiększonej liczby zadań realizowanych przez komórkę objętą sprawdzeniem może znacząco wpłynąć na jakość sprawdzenia i postrzeganie ABI w organizacji.
- Procesy realizowane okresowo – w wielu organizacjach niektóre dane są przetwarzane w określony sposób jedynie okresowo, np. w czasie wakacji. Prowadzenie sprawdzenia w czasie,

gdy przetwarzanie danych jest ograniczone, nie pozwoli stwierdzić, czy dane są przetwarzane zgodnie z zasadami.
- Możliwość wystąpienia zdarzeń powodujących, że przeprowadzenie sprawdzenia będzie wymagało dłuższego czasu (np. incydent, w związku z którym konieczne będzie rozpoczęcie sprawdzenia doraźnego).

W planie sprawdzeń ABI określa sposób i zakres dokumentowania sprawdzeń. „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." W wypadku pierwszych sprawdzeń nie ma powodu, by ABI ograniczał sobie możliwość dokumentowania sprawdzenia, tym bardziej że plan może być przygotowany kilka miesięcy przed jego rozpoczęciem. Akceptowalnym rozwiązaniem będzie wymienienie wszystkich sposobów dokumentowania sprawdzenia.

W przeciwnym wypadku okazać by się mogło, że ABI będzie miał ograniczone możliwości, np. nie będzie mógł „sporządzić kopii otrzymanego dokumentu", bo przygotowując plan sprawdzenia, nie wiedział, że w danej komórce organizacyjnej są tworzone dokumenty. Czemu służy określenie sposobu i zakresu dokumentowania sprawdzenia? W mojej ocenie chodzi o to, by pracownicy i kierownicy komórek objętych sprawdzeniem wiedzieli, jakie ABI ma uprawnienia. Przykładowo, że ABI ma prawo „odebrania wyjaśnień od osoby, której czynności objęto sprawdzeniem" czy też „sporządzenia kopii obrazu wyświetlonego na ekranie".

„Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok" (§ 3 ust. 5 rozporządzenia). Słusznie postępują ABI, którzy pierwsze plany sprawdzeń przygotowują na krócej niż rok. Jest to ciągle nowość i zarówno ABI, jak i ADO zdobywają pierwsze doświadczenia i odkrywają niuanse rozporządzenia.

Możliwa jest też zmiana już przygotowanego planu. Trzeba jedynie pamiętać, by nową wersję przedstawić administratorowi danych nie później niż na dwa tygodnie przed rozpoczęciem okresu objętego nowym planem. Z pewnością jednak zmiana planu nie będzie dobrze widziana i korzystniejsze wydaje się przygotowywanie planów na krótsze okresy. „Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat" (§ 3 ust. 6 rozporządzenia). Wymóg ten będzie szczególnie istotny w większych organizacjach. ABI powinien w taki sposób zaplanować sprawdzenia, by wszystkie systemy i zbiory danych zostały w tym okresie skontrolowane.

Sprawdzenie planowe

Pod pojęciem sprawdzenia kryją się czynności, które mają na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami. Po przeprowadzeniu sprawdzenia ABI przy-

gotowuje sprawozdanie. Powinno ono spełniać wymagania określone w art. 36c uodo. Sprawdzenia planowe prowadzone są zgodnie z przygotowanym i przedstawionym ADO planem. ABI określa w nim przedmiot, zakres i termin przeprowadzenia sprawdzeń oraz sposób i zakres ich dokumentowania. ABI musi przygotować się do przeprowadzenia sprawdzenia. Powinien np. wiedzieć, w jaki sposób będzie dokumentować sprawdzenie.

Dla części ABI sprawdzenia nie są czymś nowym. Realizując swoje zadania, prowadzili oni okresowe audity. Obecnie ABI zobowiązany będzie do prowadzenia sprawdzeń zgodnie z zasadami określonymi w rozporządzeniu. ABI mogą jednak nadal posługiwać się metodami stosowanymi z powodzeniem przez auditorów systemów zarządzania bezpieczeństwem informacji. Warto zapoznać się ze stosowanymi przez nich metodykami i normami, np.:

- PN-EN ISO 19011:2012 – Wytyczne dotyczące auditowania systemów zarządzania.
- ISO/IEC 27007:2011 – Wytyczne dotyczące auditowania systemów zarządzania bezpieczeństwem informacji (norma szeroko odnosząca się do normy ISO 19011).
- ISO/IEC TR 27008:2011 – Uzupełniający normę ISO/IEC 27007:2011 i dotyczący zabezpieczeń technicznych, zwłaszcza w obszarze bezpieczeństwa IT.

Prowadząc sprawdzenie, ABI powinien mieć na uwadze, że jego celem jest weryfikacja zgodności przetwarzania danych osobowych. Jak więc powinien postąpić, jeżeli w trakcie sprawdzenia uzna, że stosowane zabezpieczenia są zgodne z opisanymi w Polityce bezpieczeństwa, jednak niewystarczające. ABI może również w trakcie sprawdzenia sprawować nadzór nad opracowaniem i aktualizowaniem dokumentacji. Chodzi w szczególności o Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym. Środki techniczne i organizacyjne powinny zapewniać ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W przypadku stwierdzenia niewystarczających zabezpieczeń ABI powinien podjąć niezbędne działania.

Nie każdy ABI ma wiedzę i umiejętności pozwalające mu na samodzielne sprawdzanie zabezpieczeń systemu informatycznego. Jednak w ramach sprawdzenia powinien upewnić się, że zabezpieczenia techniczne zostały prawidłowo dobrane, są monitorowane i testowane. Jeżeli ABI nie ma odpowiedniej wiedzy, powinien zapewnić sobie wsparcie osób, które ją posiadają. Istotna będzie krzyżowa weryfikacja oświadczeń użytkowników i administratorów systemów.

Ważne

ABI nie powinien polegać na oświadczeniu administratora systemów informatycznych (ASI), że zgodnie z dokumentacją system wymusza zmianę hasła co 30 dni. Powinien dodatkowo zapytać użytkowników, jak często zmieniają hasła i czy system o tym przypomina.
ABI nie powinien też polegać na oświadczeniu ASI, że użytkownicy mają ograniczone uprawnienia w systemie, ale zapytać ich, jakie to są uprawnienia. ABI powinien również poprosić użytkowników i administratorów, aby zademonstrowali mu te czynności.

Dobrą praktyką jest, aby osoba sprawdzająca nie wykonywała powyższych czynności samodzielnie. Zostało to również uwzględnione w rozporządzeniu, zgodnie z którym: „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”**.** Nie oznacza to, że ABI, który ma odpowiednią wiedzę, nie może przeprowadzić testów bezpieczeństwa systemu informatycznego. Powinno to jednak zostać wskazane w planie sprawdzeń, a same czynności muszą być bardzo dokładnie dokumentowane.

Lista kontrolna to proste, często stosowane narzędzie, które pozwala na uporządkowanie informacji zbieranych w trakcie sprawdzenia. Ułatwia pracę prowadzącemu sprawdzenie i zapewnia, że żaden z obszarów nie zostanie pominięty. Lista kontrolna może zawierać pytania, które ABI zada w trakcie sprawdzenia, i powinna być zgodna z określonym w planie sprawdzeń zakresem sprawdzenia. Przygotowując listę pytań, ABI uwzględni wszystkie wymogi ustawy i rozporządzeń, jak również obowiązki wynikające z wewnętrznej dokumentacji (Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym). Dobrą praktyką jest samodzielne przygotowanie listy pytań. Posłużenie się znalezioną gdzieś w Internecie przykładową listą może doprowadzić do sytuacji, gdy ABI nie będzie rozumiał zadanego pytania, co z pewnością zostanie zauważone przez osoby objęte sprawdzeniem. Praktykuje się również przygotowanie specjalnej listy kontrolnej dla osób, z którymi będą następnie prowadzone wywiady.

Efekty sprawdzenia zależą od współpracy z osobami, których czynności podlegają sprawdzeniu, i które będą nam udzielać informacji. Istotne będzie wyjaśnienie im celu sprawdzenia i zwrócenie uwagi, że dążymy do udoskonalenia działania systemu ochrony danych, a nie szukamy osób odpowiedzialnych za nieprawidłowości.

Ważne

Jak prowadzić rozmowy – przydatne wskazówki

Stosujmy pytania otwarte. Jeżeli zapytamy pracownika „Czy zmienia Pan hasło co 30 dni?”, prawdopodobnie otrzymamy odpowiedź – „Tak”. Zapytajmy „Co ile dni zmienia Pan hasło?”. Dowiemy się, czy pracownik zna obowiązującą go procedurę.

Unikajmy pytań sugerujących odpowiedź. Zamiast pytać, gdzie są przechowywane klucze do szaf, poprośmy, aby pracownik krok po kroku opisał nam, w jaki sposób postępuje na koniec dnia pracy. Możemy dodatkowo poprosić o pokazanie zawartości wybranej szafy – zobaczymy, gdzie naprawdę pracownicy przechowują klucze.

Zadawajmy pytania „krzyżowe” – np. pytajmy o to samo administratorów i użytkowników systemów. Rozmawiajmy nie tylko z kierownikami, ale również z pracownikami operacyjnymi. To oni wiedzą najlepiej, jak w rzeczywistości realizowane są procedury.

Warto również, by zarząd przekazał taką deklarację kierownikom poszczególnych komórek organizacyjnych. W praktyce spotykamy się z sytuacją, gdy kierownicy instruują pracowników, jakie informacje mają przekazywać auditorom. Doświadczony ABI wychwyci takie sytuacje.

Zgodnie z rozporządzeniem „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". Dobrą praktyką jest zbieranie kopii dokumentów, o których rozmawiamy w trakcie sprawdzenia. Rozporządzenie określa, na czym może polegać dokumentowanie. Jest to katalog otwarty, w razie potrzeby może być rozszerzony o:

1. **Notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych.**

Notatki stanowią zwykle podstawę pracy prowadzącego sprawdzenie administratora bezpieczeństwa informacji. Powinien on odnotowywać wszelkie istotne informacje. Notatki mogą być sporządzane w formie elektronicznej (tablet, laptop) lub w formie papierowej. Od ich jakości zależeć będzie jakość przygotowanego sprawozdania. Notatki powinny być wystarczająco szczegółowe. Zawsze notujmy dane osoby, która udzieliła informacji, datę i godzinę spotkania. Jeżeli notatka dotyczy oględzin pomieszczenia, powinna wskazywać, którego pomieszczenia dotyczy, oraz zawierać szczegółową informację o poddanych oględzinom elementach. Jeżeli ABI stwierdzi pozostawiony w zamku szafy klucz, powinien wskazać, której szafy to dotyczy i jakie dokumenty się w niej znajdują. Pozwoli to uniknąć podważających jego wiarygodność sytuacji, gdy po wskazaniu w sprawozdaniu nieprawidłowości okaże się, że szafa nie służy do przechowywania żadnych danych.

2. **Wyjaśnienia osoby, którą objęto sprawdzeniem.**

Wyjaśnienia mogą być zebrane również na piśmie. Dotyczyć to może zwłaszcza tych sytuacji, gdy ABI stwierdza nieprawidłowości, nie ma możliwości osobistego zapoznania się z sytuacją albo istnieje podejrzenie wystąpienia konfliktu interesów.

3. **Kopie dokumentów.**

Dobrą praktyką będzie zbieranie kopii wszystkich dokumentów, w miarę możliwości jednak nie powinny one zawierać danych osobowych.

4. **Zrzuty ekranów.**
5. **Rejestry systemu, konfiguracje systemu.**

Sprawdzenie doraźne

Oprócz sprawdzeń przewidzianych w planie sprawdzeń, w wypadku naruszenia ochrony danych lub uzasadnionego podejrzenia wystąpienia takiego naruszania, ABI może przeprowadzić sprawdzenia doraźne. Administrator bezpieczeństwa informacji rozpoczyna sprawdzenie doraźne, jeżeli otrzyma informację o naruszeniu ochrony danych osobowych, lub podejrzeniu takiego naruszenia. Jednym z podstawowych problemów, jaki się pojawia, jest konieczność rozstrzygnięcia czy należy rozpocząć sprawdzenie doraźne, czy wystarczające będzie podjęcie działań w ramach prowadzonej weryfikacji.

Sprawując nadzór ABI m.in. prowadzi weryfikację stanu faktycznego w zakresie przetwarzania danych osobowych oraz zgodności ze stanem faktycznym przewidzianym w dokumentacji zabezpieczeń technicznych i organizacyjnych. ABI prowadzi weryfikację poza sprawdzeniami

na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych oraz własnego udziału w procedurach w niej określonych, a także na podstawie zgłoszenia osoby trzeciej. Sprawdzenie doraźne jest prowadzone w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.

Dlatego, ABI musi rozstrzygnąć, czy ma do czynienia z naruszeniem ochrony danych osobowych, czy też inną nieprawidłowością. Niestety, brak w ustawie i rozporządzeniu jednoznacznej definicji, kiedy mamy do czynienia z naruszeniem ochrony danych, oznaczającym konieczność rozpoczęcia sprawdzenia doraźnego. A dopuszczenie prowadzenia weryfikacji, na podstawie zgłoszeń, poza sprawdzeniami wyraźnie sugeruje, że nie w każdym wypadku, będziemy mieli do czynienia z koniecznością wszczynania sprawdzenia. O naruszeniu ochrony danych osobowych zapewne powiemy w wypadku „wycieku" danych, gdy zostaną one ujawnione osobom nieupoważnionym. W innych sytuacjach możemy przyjąć podejście uwzględniające końcowy efekt.

Jeżeli w ocenie ABI, wystarczające będzie zakończenie działań pouczeniem, poinstruowaniem i ewentualnie powiadomieniem ADO, ABI może ograniczyć się do przeprowadzenia weryfikacji. Jeżeli jednak naruszenie ochrony danych będzie wymagało podjęcia dalej idących działań i opracowania sprawozdania, ABI powinien bez zbędnej zwłoki rozpocząć sprawdzenie doraźne.

Sprawozdania z przeprowadzonych sprawdzeń służą nie tylko do przekazania informacji administratorowi danych, ale są również narzędziem gromadzenia wiedzy w organizacji. Organizacja może z niej korzystać w przyszłości dla uniknięcia powtarzania tych samych błędów. ABI powinien natomiast weryfikować, skuteczność podjętych i realizację planowanych działań, które wskazał w sprawozdaniach.

Sam przebieg sprawdzenia doraźnego nie różni się zasadniczo od przebiegu sprawdzenia prowadzonego zgodnie z planem sprawdzeń. Najważniejsze różnice to:

1. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez administratora bezpieczeństwa informacji o naruszeniu ochrony lub uzasadnionym podejrzeniu naruszenia.
2. Jeszcze przed podjęciem pierwszej czynności w toku sprawdzenia doraźnego, ABI zawiadamia administratora danych o jego rozpoczęciu.
3. Jeżeli niezwłoczne rozpoczęcie sprawdzenia doraźnego jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce, administrator bezpieczeństwa informacji nie jest zobowiązany do wcześniejszego zawiadomienia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności.

Zauważmy pewien brak spójności. Sprawdzenie powinno być przeprowadzone niezwłocznie. Z drugiej strony, kierownika jednostki organizacyjnej nie informujemy o rozpoczęciu spraw-

dzenia, tylko wtedy, gdy „niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem (…)".

ABI powinien rozpocząć sprawdzenie niezwłocznie, a dopiero gdy dokona oceny, że podjęcie kolejnych działań nie jest niezwłocznie niezbędne, może poinformować kierownika jednostki organizacyjnej o terminach kolejnych działań.

Prowadzący sprawdzenie ABI, dokumentuje przeprowadzone czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania. Nie różni się to zasadniczo od działań podejmowanych w czasie sprawdzenia prowadzonego zgodnie z planem.

Ponieważ jednak sprawdzenie doraźne będzie niejednokrotnie wszczynane w związku z poważnym incydentem, który może wiązać się nawet z ewentualnym przestępstwem, ABI powinien zbierać dowody audytowe wyjątkowo skrupulatnie. Jeżeli uzna on, że nie posiada wystarczających kwalifikacji do np. analizy naruszenia bezpieczeństwa systemu informatycznego, powinien wziąć pod uwagę skorzystanie z usług osoby lub zewnętrznego podmiotu posiadającego odpowiednie kwalifikacje (eksperta technicznego). Należy jednak zwracać uwagę na ewentualne konflikty interesów (przykładowo ekspert techniczny będący pracownikiem podmiotu, który konfigurował skompromitowane w czasie incydentu zabezpieczenia sieci).

Dokumentując sprawdzenie ABI może uwzględnić:
1. Notatki z czynności, zebranych wyjaśnień, przeprowadzonych oględzin.
2. Wyjaśnienia osoby, której czynności objęto sprawdzeniem.
3. Kopie dokumentów.

Dobrą praktyką będzie zbieranie kopii wszystkich dokumentów, w miarę możliwości jednak, nie powinny one zawierać danych osobowych.

4. Zrzuty ekranów.
5. Rejestry systemu (logi, dzienniki zdarzeń), konfiguracje systemu.

Jednocześnie ABI podejmuje działania niezbędne dla usunięcia nieprawidłowości. I w tym wypadku działania mogą znacząco różnić się od tych podejmowanych w trakcie sprawdzenia planowego. Sprawdzenie doraźne będzie często podejmowane w razie wystąpienia nieoczekiwanego incydentu o dużej skali i istotnym znaczeniu dla organizacji.

Część z nich będzie się wiązała z koniecznością zaangażowania najwyższego kierownictwa organizacji oraz współdziałania z innymi osobami, np. odpowiedzialnymi za przekazywanie informacji opinii publicznej lub osobom, których prywatność mogła być naruszona. Od administratora bezpieczeństwa informacji będą tu wymagane działania chroniące interes organizacji, bez naruszania interesu osób, których ochrona danych została naruszona.

Istotne wydaje się wdrożenie procedur, które zapewnią, że ABI jak najszybciej otrzyma informację, na podstawie której będzie mógł rozpocząć sprawdzenie. Należy również opracować procedury pozwalające administratorowi bezpieczeństwa informacji, bez zbędnej zwłoki poinformować administratora danych o rozpoczęciu sprawdzenia. Musimy zabezpieczyć się przed sytuacją, w której ABI nie będzie mógł prowadzić sprawdzenia doraźnego, tylko dlatego, że nie może poinformować ADO o jego rozpoczęciu. Tworzące te procedury warto zajrzeć do norm. Zwłaszcza norma ISO/IEC 27035 — „Information technology — Security techniques — Information security incident management", może pomóc w klasyfikacji incydentów i wprowadzeniu zasad postępowania z poszczególnymi kategoriami incydentów.

Sprawozdanie ze sprawdzenia planowego i doraźnego

Jednym z wymienionych w ustawie o ochronie danych osobowych obowiązków ABI jest przygotowanie sprawozdania z przeprowadzonego sprawdzenia. Sprawozdanie należy sporządzić bez względu na rodzaj sprawdzenia – dla sprawdzenia planowego, doraźnego oraz sprawdzenia, o przeprowadzenie którego zwrócił się GIODO. Sprawozdanie jest bardzo ważnym elementem pracy administratora bezpieczeństwa informacji. Dokumentuje ono realizację obowiązku prowadzenia sprawdzeń i jest końcowym elementem ciągu czynności: plan sprawdzeń – sprawdzenie – sprawozdanie. Od jakości sprawozdania zależeć będzie, czy praca włożona w przeprowadzenie sprawdzenia odniesie pozytywny skutek i przełoży się na zapewnienie zgodnego z prawem przetwarzania danych osobowych w organizacji.

Sposób realizacji większości zadań administratorów bezpieczeństwa informacji określony został w rozporządzeniu ministra administracji i cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji. Jednak elementy, które powinno zawierać sprawozdanie, zostały określone w ustawie o ochronie danych osobowych. Sprawozdanie przygotowywane jest przez ABI dla administratora danych. Jeżeli ABI nie zostanie powołany, jego zadania realizowane są przez administratora danych, nie ma on jednak obowiązku przygotowania sprawozdania ze sprawdzenia.

Ważne

O przeprowadzenie sprawdzenia może zwrócić się do wpisanego do rejestru administratora bezpieczeństwa informacji również Generalny Inspektor Ochrony Danych Osobowych. Wskaże on wówczas zakres i termin sprawdzenia. Administrator bezpieczeństwa informacji przedstawi GIODO sprawozdanie z tego sprawdzenia za pośrednictwem administratora danych osobowych. Z pewnością jest to jeden z trudniejszych momentów w karierze ABI, gdy musi za pośrednictwem administratora danych przedstawić sprawozdanie ze sprawdzenia, które być może zawiera informacje o stwierdzonych u administratora nieprawidłowościach. Stanowi to jednocześnie test pozycji ABI w organizacji, gdyż administrator danych powinien uszanować organizacyjną niezależność ABI i nie ingerować w treść sprawozdania.

Administrator bezpieczeństwa informacji zobowiązany jest przekazać sprawozdanie ze sprawdzenia w terminie:

- ze sprawdzenia planowego – nie później niż 30 dni od zakończenia sprawdzenia,
- ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia,
- ze sprawdzenia, o którego dokonanie zwrócił się GIODO – zachowując termin wskazany przez GIODO.

Wymagane elementy sprawozdania określone zostały w art. 36c ustawy o ochronie danych osobowych:

- oznaczenie administratora danych osobowych i adres jego siedziby lub miejsca zamieszkania, imię i nazwisko administratora bezpieczeństwa informacji;

Pierwsze wymagane elementy sprawozdania mają charakter porządkowy i stanowią wskazanie administratora danych i administratora bezpieczeństwa informacji. Konieczność zawarcia tych elementów w sprawozdaniu staje się jasna, gdy zwrócimy uwagę, że sprawozdanie może być również przygotowane dla GIODO.

- wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;

Przygotowujący sprawozdanie ABI powinien wskazać czynności podjęte podczas sprawdzenia. Zgodnie z § 4 rozporządzenia, ABI już w trakcie prowadzenia sprawdzenia dokumentuje podejmowane czynności, dlatego sporządzenie ich wykazu nie powinno być problemem.

Ważnym elementem jest wskazanie osób biorących udział w tych czynnościach. Będzie to bardzo przydatne na etapie realizacji zaleceń ze sprawdzenia, gdy niezbędne okaże się wskazanie osób, od których ABI otrzymał wyjaśnienia, dokumenty, wydruki itd.

- data rozpoczęcia i zakończenia sprawdzenia;

Powinniśmy wskazać rzeczywiste daty rozpoczęcia i zakończenia sprawdzenia. Również wtedy, jeżeli z jakiegoś powodu będą one odbiegały od dat wskazanych w planie sprawdzeń.

- określenie przedmiotu i zakresu sprawdzenia;

Wskazujemy przedmiot i zakres sprawdzenia – analogicznie, jak czyniliśmy to w planie sprawdzeń, z tym że wskazujemy tutaj rzeczywisty, zrealizowany zakres sprawdzenia. Okazać się może, że nie było możliwe przeprowadzenie sprawdzenia w zakresie wskazanym w planie sprawdzeń. Dobrą praktyką będzie wówczas poinformowanie o tym w dalszej części sprawozdania oraz uwzględnienie pominiętych obszarów w kolejnych planach sprawdzeń.

- opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie da-

nych osobowych;

Punkt ten jest jedną z istotniejszych części sprawozdania. Opis powinien być jednoznaczny i pełny, jednak pozbawiony zbędnych dla odbiorcy informacji. Przykładowo, w sprawozdaniu kierowanym do administratora danych możliwe będzie pominięcie informacji, które będą niezbędne w sprawozdaniu przygotowywanym dla Generalnego Inspektora Ochrony Danych Osobowych.

- stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;

W punkcie tym podajemy:
Wszystkie stwierdzone w czasie auditu przypadki naruszenia przepisów o ochronie danych osobowych. Pamiętajmy jednak, że odbiorca sprawozdania nie musi być specjalistą w dziedzinie ochrony danych osobowych – wyjaśnijmy w tym punkcie, na czym naruszenie polega i z jakimi zagrożeniami się wiąże.

Zgodnie z § 8 rozporządzenia, sprawozdanie może zawierać również:
- Zawiadomienie 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 ABI może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności).
- Zawiadomienie administratora danych o nieaktualności dokumentacji przetwarzania danych. ABI może przedstawić administratorowi danych do wdrożenia projekty dokumentów aktualizujących.
- Informacje o podjętych działaniach przywracających stan zgodny z prawem.

Jeżeli w trakcie sprawdzenia zostaną niezwłocznie podjęte działania przywracające stan zgodny z prawem, powinny zostać wskazane w tym punkcie sprawozdania.
- Informacje o planowanych działaniach przywracających stan zgodny z prawem.

Jest to jeden z budzących najwięcej wątpliwości punktów sprawozdania. To, jakie działania zostaną podjęte, niejednokrotnie nie będzie zależało od decyzji ABI. Ponadto, ABI przygotowuje sprawozdanie ze sprawdzenia, a nie sprawozdanie z działań podejmowanych w celu przywrócenia stanu zgodnego z prawem, co z oczywistych powodów może trwać dłużej niż czas, który ma ABI na przedstawienie sprawozdania.

Wydaje się, że w takiej sytuacji ABI powinien opisać, jakie działania już zostały podjęte (np. że oczekuje na decyzję zarządu, co do dalszych działań), a jeżeli działania nie zostały jeszcze podjęte, ABI może przedstawić propozycję działań przywracających stan zgodny z prawem.
- wyszczególnienie załączników stanowiących składową część sprawozdania;

Podajemy listę załączników sprawozdania. Mogą to być wszelkiego rodzaju zebrane w trakcie sprawdzenia dokumenty, wyjaśnienia, opinie prawne itp.

- podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania, datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.

W wypadku sprawozdania składanego w postaci papierowej ABI podpisuje sprawozdanie i dodatkowo składa parafy na każdej stronie sprawozdania. Problem pojawia się w wypadku sprawozdania składanego w formie elektronicznej. Niestety, wydaje się, że zgodnie z ustawą o podpisie elektronicznym jedyną akceptowalną obecnie formą podpisu będzie bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu (potocznie zwany podpisem kwalifikowanym).

ABI powinien zastanowić się, do kogo kieruje sprawozdanie i dostosować użyty w nim język do odbiorcy. Używanie w treści niezrozumiałych dla odbiorcy pojęć informatycznych, prawniczych czy nawet z dziedziny ochrony danych osobowych może spowodować, że odbiorca nie poświęci problemom wskazanym w sprawozdaniu wystarczającej uwagi. Z kolei dobrze napisane sprawozdanie, poruszające istotne dla organizacji problemy i proponujące korzystne dla organizacji rozwiązania może w istotny sposób przyczynić się do podniesienia poziomu ochrony danych osobowych w organizacji.

1 NUMER PRAWNICZY RAZ NA KWARTAŁ, przygotowany przez Kancelarię Prawną Traple, Konarski, Podrecki i Wspólnicy

OCHRONA DANYCH OSOBOWYCH
profesjonalnie i kompleksowo

W MIESIĘCZNIKU ZNAJDZIESZ:

- ✔ **gotowe, w pełni edytowalne wzory dokumentów** związanych z przetwarzaniem danych osobowych wraz z instrukcjami wypełnienia krok po kroku,
- ✔ **przykładowe zapisy umowne**,
- ✔ **wyjaśnienie zawiłych kwestii prawnych**, w szczególności na styku ochrony danych osobowych i nowych technologii,
- ✔ **porady, jak zachować się podczas kontroli GIODO**,
- ✔ **zmiany w prawie i ich konsekwencje** dla pracy ABI, ADO i ASI,
- ✔ **szczegółowe porady na temat danych osobowych** dla firm prywatnych oraz administracji publicznej,
- ✔ **gotowe materiały do przeprowadzania szkoleń** z zakresu danych osobowych.

Zamów prenumeratę!

1 **Półroczną z 20% zniżką**
+ myszka gratis

2 **Roczną z 30% zniżką**
+ tablet gratis

Zamów prenumeratę już dziś na FabrykaWiedzy.com,
lub przez Centrum Obsługi Klienta: **tel. 22 518 29 29, email: cok@wip.pl**

1BK61

ISBN: 978–83–269–5431–3