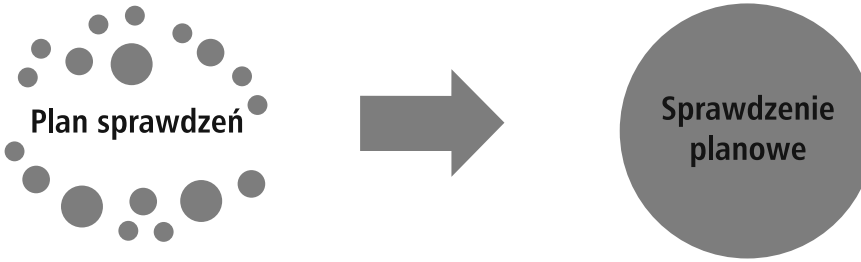
Tworzenie systemu ochrony danych osobowych wymaga przeprowadzenia analizy poszczególnych wymogów obecnie obowiązującego prawa, jak również tych przepisów, które zaczną obowiązywać w roku 2018. Stworzenie planu działania jest kluczem do skutecznego wdrożenia systemu bezpieczeństwa danych osobowych. Poszczególne wymogi powinny zostać spełnione w odpowiedniej kolejności, tak by nie powodować chaosu w organizacji. Dodatkowo powinniśmy pamiętać o zasobach potrzebnych do stworzenia systemu ochrony danych, tj. zasobach ludzkich, środkach finansowych i dostępnych obszarach przetwarzania.

Sprawdzenie systemu ochrony danych

System ochrony danych osobowych, podobnie jak każdy wewnętrzny system reguł postępowania, w określonych sytuacja wymaga okresowej weryfikacji. Musi być ona dokonywana systematycznie (obecnie obowiązuje okres jednego roku jako maksymalny przedział czasowy[27]), gdyż każda organizacja zmienia się wraz z upływem czasu, stosuje coraz nowsze technologie przy przetwarzaniu danych osobowych, upraszcza procesy ich przetwarzania, a niekiedy gromadzi więcej danych o osobach, których dane dotyczą. Głównym zadaniem ABI w organizacji są obecnie sprawdzenia systemu ochrony danych osobowych podzielone na trzy kategorie wewnętrzne: sprawdzenia planowe, doraźne i na żądanie GIODO. Jedynie poprzez okresowe sprawdzenia ABI można w sposób obiektywny dowiedzieć się, jak faktycznie są przetwarzane w organizacji dane osobowe oraz czy zidentyfikowany sposób przetwarzania danych jest zgody z treścią wewnętrznej dokumentacji ochrony danych osobowych. Obowiązujący aktualnie cykl sprawdzeń charakteryzuje się sporym formalizmem.

[27] Par. 3 ust. 5 rozporządzenia 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 (Dz.U. poz. 745).



- **14 dni** przed pierwszą czynnością objętą planem – informacja do administratora danych
- **7 dni** przed pierwszą czynnością objętą planem – informacja do kierownika jednostki organizacyjnej podlegającej sprawdzeniu

- **30 dni** na przygotowanie sprawozdania ze sprawdzenia planowego oraz jego dostarczenie do administratora danych
- Przygotowanie kolejnego planu sprawdzeń na następny okres nie mniejszy niż kwartał i nie większy niż rok

Rys. 5. Terminy sprawdzeń planowych
Źródło: oprac. autora.

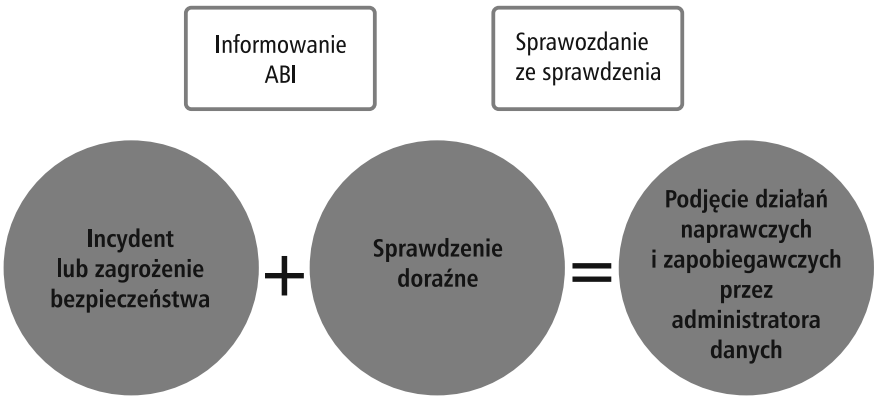
Inspektor ochrony danych również musi realizować zadania sprawdzające i audytowe, jednak rozporządzenie ogólne UE nie określa szczegółowo, jak taki proces ma wyglądać, należy więc założyć, że pozostanie tu pewna doza dowolności co do tego, jakimi metodami będą przeprowadzane audyty oraz w jakich odstępach czasu będą dokonywane.

„Inspektor ochrony danych ma następujące zadania:
[…]
monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz **polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty; […]”**[28].

[28] Art. 39 ust. 1 pkt b rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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).

Powyższe zadania są bardzo zbliżone do zadań obecnie funkcjonującego ABI. Pozwoli to z pewnością na stosunkowo płynne przejście z obecnego rygoru prawnego do bardziej dowolnego kształtowania cyklu sprawdzeń. Każde sprawozdanie ze sprawdzenia systemu ochrony danych osobowych (nawet jeżeli sprawdzenie nie wykaże żadnych niezgodności z przepisami prawa) powinno uwzględniać ciągłe doskonalenie tego systemu. Warto pamiętać, że obecnie obowiązujący przedział czasowy pomiędzy sprawdzeniami – czyli rok – to wystarczająco dużo, by osoby przetwarzające dane osobowe zdążyły zapomnieć o ryzykach, jakie wiążą się z przetwarzaniem danych osobowych lub aby po prostu powstały nowe ryzyka. Podobnie rzecz ma się z podmiotami zewnętrznymi, którym powierzono przetwarzanie danych osobowych. Istnieje duże prawdopodobieństwo, że także w tych podmiotach osoby odpowiedzialne za przestrzeganie obowiązków wynikających z umów powierzenia przetwarzania danych osobowych zapomną o nich lub po prostu przestaną chronić powierzone dane w celu ograniczenia kosztów. Mówiąc inaczej, w przypadku większości organizacji roczny cykl sprawdzeń wydaje się optymalnym rozwiązaniem dla sprawdzenia systemu ochrony danych osobowych.

Nieco innym rodzajem sprawdzeń są tzw. sprawdzenia doraźne czy też incydentalne. ABI musi przeprowadzić sprawdzenie, gdy dojdzie do incydentu lub nawet samego zagrożenia danych osobowych. Celem przeprowadzania tej kategorii sprawdzeń jest przede wszystkim podjęcie szybkich działań naprawczych i zapobiegawczych przez administratora danych. Jednak możliwe jest to dopiero wtedy, gdy incydent lub zagrożenie będzie ostatecznie zidentyfikowane.



Rys. 6. Cykl sprawdzeń doraźnych
Źródło: oprac. autora.

W ramach incydentów ochrony danych osobowych rozporządzenie ogólne UE nakłada dodatkowe obowiązki, jednak dotyczą one samego administratora danych, a nie inspektora ochrony danych. Konkretnie jest to obowiązek zawiadomienia organu nadzorczego – GIODO – nie później nie po upływie 72 godzin.

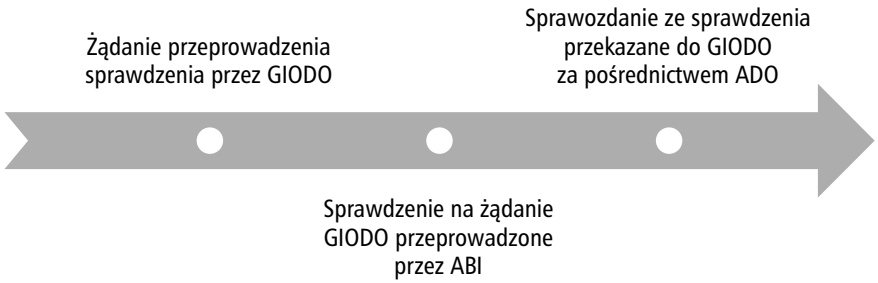
> „W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia”[29].

Ostatecznie może dojść do sytuacji, w której GIODO postanowi zweryfikować zgodność przetwarzania danych osobowych w konkretnej organizacji. Może wówczas wystąpić z żądaniem przeprowadzenia

[29] Art. 33 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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).

sprawdzenia przez ABI oraz z żądaniem przesłania sprawozdania z tego sprawdzenia.

„Generalny Inspektor może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c, o dokonanie sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia. Po dokonaniu sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, administrator bezpieczeństwa informacji, za pośrednictwem administratora danych, przedstawia Generalnemu Inspektorowi sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a"[30].



Rys. 7. Sprawdzenie na żądanie GIODO – etapy procesu
Źródło: oprac. autora.

Podsumowując, sprawdzenia systemu ochrony danych osobowych (obecnie obowiązujące, jak i te, których obowiązek przeprowadzania pojawia się na mocy rozporządzenia ogólnego UE) pozostaną obowiązkiem ABI lub IOD. Jest to główna metoda utrzymywania stanu ochrony danych osobowych w organizacji w ciągłej zgodności z przepisami prawa oraz sukcesywnego doskonalenia bezpieczeństwa informacji w organizacji.

Modyfikacja systemu ochrony danych

Podstawą do wprowadzania zmian w systemie ochrony danych osobowych są sprawozdania ze sprawdzeń. Z tego też względu muszą one zawierać rekomendacje mające na celu poprawę. Aby jednak właści-

30 Art. 19b ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.).