Jak stworzyć instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

experto24.pl
TWÓJ OSOBISTY DORADCA

Jak stworzyć instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Instrukcja zarządzania systemem informatycznym to obok polityki bezpieczeństwa podstawowy dokument, jaki każda jednostka przetwarzająca dane osobowe powinna stworzyć. Przepisy podpowiadają jak to zrobić, jednak nie można ograniczyć się do przepisania zapisów z rozporządzenia.

Obowiązek przygotowania instrukcji zarządzania systemem informatycznym wynika z rozporządzenia ministra spraw wewnętrznych i administracji z 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 1 maja 2004 r.).

Instrukcja – obowiązek ADO

Do opracowania i wdrożenia instrukcji zobowiązani są wszyscy administratorzy danych osobowych, przetwarzający dane z wykorzystaniem systemu informatycznego. W praktyce, jest to niemal każdy administrator danych.

Systemy informatyczne zmieniają się bardzo szybko. Rozporządzenie z 2004 roku z pewnością nie przystaje do tych współczesnych i nie uwzględnia aktualnych zagrożeń bezpieczeństwa danych. Jednak wciąż obowiązuje i wszyscy administratorzy danych zobowiązani są do stosowania się do jego wymagań.

UWAGA!

Wymagania określone w rozporządzeniu są minimalne. Każdy z administratorów powinien dobrać zabezpieczenia adekwatne do zagrożeń i kategorii danych, jakie występują w jego podmiocie. Nie można ograniczyć się jedynie do wdrożenia zabezpieczeń wymienionych w rozporządzeniu.

Więcej niż wymaga prawo

Rozporządzenie mówi, jakie elementy są wymagane w instrukcji. Nie oznacza to, że nie powinny znaleźć się w niej inne procedury. Instrukcja nie powinna być przepisanym rozporządzeniem. Trzeba możliwie szczegółowo opisać faktycznie obowiązujące procedury wymienione w rozporządzeniu. Przykładami dodatkowych procedur mogą być: „Procedura prowadzenia ewidencji sprzętu i oprogramowania", „Procedura zmiany konfiguracji systemu", „Procedura prowadzenia testów nowych wersji systemu", „Zasady prowadzenia szkoleń w zakresie bezpieczeństwa informacji", itd.

PRZYKŁAD

Błędem przy tworzeniu instrukcji jest np. ograniczenie się w procedurze nadawania uprawnień, do stwierdzenia typu **„Nadaje się uprawnienia do systemu informatycznego"**. Należy szczegółowo opisać kolejne kroki, przewidzieć sytuacje nietypowe oraz wskazać osoby odpowiedzialne. Przykładowo, jeżeli uprawnienia nadaje administrator systemu, to powinniśmy to napisać. Może to wyglądać w taki sposób: „ABI przekazuje kopię upoważnienia administratorowi systemu kadrowo-płacowego, który tworzy konto użytkownika oraz wprowadza uprawnienia w zakresie zgodnym z upoważnieniem".

Tworzenie procedur możemy rozpocząć od przeprowadzenia wywiadów i opisania rzeczywiście funkcjonujących w organizacji toków postępowania. Musimy jednak je przeanalizować i upewnić się, że zapewniają one odpowiedni poziom bezpieczeństwa. Musimy uwzględnić wymagania biznesowe organizacji. Pamiętajmy jednak, że ograniczenia organizacyjne i finansowe nie mogą uzasadniać niezgodnego z prawem przetwarzania danych.

Struktura dokumentu

Czasami tworzoną dokumentację należy podzielić na kilka części, lub przygotować wersje dla osób pracujących na różnych stanowiskach czy w różnych działach. Należy ją przygotować w taki sposób, by każdy z użytkowników systemu informatycznego miał możliwość zapoznania się z obowiązującymi go procedurami.

Dokumentacja nie powinna jednak obniżać poziomu bezpieczeństwa danych, dlatego nie udostępniajmy użytkownikom tych informacji, które nie są im niezbędne. Przykładowo, nie każdy pracownik powinien wiedzieć, gdzie są przechowywane kopie bezpieczeństwa.

Zarówno instrukcja, jak i polityka bezpieczeństwa powinny być dokumentami stale aktualizowanymi. Należy uwzględniać w

nich zmiany organizacyjne, modyfikacje systemów informatycznych oraz pojawiające się nowe zagrożenia.

Podstawowe elementy instrukcji zarządzania systemem informatycznym

Element wymagany zgodnie z § 5 rozporządzenia	Właściwa zawartość instrukcji
1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;	Procedury, które tworzymy powinny obejmować: • nadawanie uprawnień dla nowych pracowników, • modyfikacje uprawnień spowodowane zmianą stanowiska pracy, • modyfikacje uprawnień spowodowane zmianą wersji oprogramowania, • odebranie uprawnień zwalnianego użytkownika systemu (zastanówmy się, czy przypadkiem uprawnienia nie powinny być odebrane, zanim pracownik dowie się, że został zwolniony?), • odebranie uprawnień użytkownikowi systemu, który porzucił pracę, • sposób postępowania na wypadek nieobecności administratora systemu, • sposób okresowego przeglądu uprawnień, • oraz inne, specyficzne dla organizacji przypadki. Zawsze należy wskazać, kto odpowiada za wykonanie poszczególnych czynności. W procedurach należy opisać, w jaki sposób będzie tworzony i przekazywany użytkownikowi identyfikator. Niezależnie należy stworzyć procedury dotyczące kont administracyjnych. W procedurach musimy uwzględnić wszystkie systemy wykorzystywane do przetwarzania danych. Możemy tworzyć osobne

	procedury dla poszczególnych systemów, lub uwzględnić kilka systemów w jednej procedurze.
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;	Opisujemy stosowane metody i środki uwierzytelnienia. Jeżeli do logowania użytkownicy wykorzystują hasła, opisujemy jak zapewnimy stosowanie haseł o wymaganej przez rozporządzenie złożoności oraz okresową zmianę hasła (wskazujemy, czy jest to wymuszane przez system, czy też użytkownik musi o tym pamiętać samodzielnie). Należy opisać sposób, w jaki użytkownikowi zostanie przekazane pierwsze hasło, oraz sposób postępowania na wypadek zapomnienia hasła. Jeżeli do uwierzytelniania wykorzystywane są inne niż hasło mechanizmy (np. karty procesorowe), również należy opisać stosowane procedury (metodę personalizacji kart, sposób postępowania na wypadek zapomnienia kodu PIN, itd.).
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;	Tworzymy procedury opisujące sposób rozpoczęcia (włączenie komputera, logowanie do systemu, itd.) i zakończenia pracy w systemie przez użytkownika. Należy stworzyć procedurę postępowania na wypadek zawieszenia pracy (np. przy chwilowym opuszczeniu stanowiska pracy). Procedura może zobowiązać użytkownika do wylogowania się z systemu, ale może też nakazać mu jedynie zablokowanie stacji. Jeżeli wykorzystujemy mechanizmy automatycznego blokowanie stacji w razie oddalenia się użytkownika, należy je również opisać. Procedury powinny uwzględniać sposób postępowania na wypadek problemów z logowaniem lub podejrzenia naruszenia bezpieczeństwa.

	Tworzymy procedury opisujące sposób rozpoczęcia (włączenie komputera, logowanie do systemu, itd.) i zakończenia pracy w systemie przez użytkownika. Należy stworzyć procedurę postępowania na wypadek zawieszenia pracy (np. przy chwilowym opuszczeniu stanowiska pracy). Procedura może zobowiązać użytkownika do wylogowania się z systemu, ale może też nakazać mu jedynie zablokowanie stacji. Jeżeli wykorzystujemy mechanizmy automatycznego blokowanie stacji w razie oddalenia się użytkownika, należy je również opisać. Procedury powinny uwzględniać sposób postępowania na wypadek problemów z logowaniem lub podejrzenia naruszenia bezpieczeństwa.
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;	Opisujmy szczegółowo procedury wykonywania kopii zapasowych. Powinny być możliwie szczegółowe i zawierać takie elementy jak: • wskazanie zbiorów danych znajdujących się w poszczególnych kopiach, • harmonogram wykonywania kopii poszczególnych zasobów, • częstotliwość wykorzystywania poszczególnych nośników, • okres czasu lub ilość wykonanych kopii, po którym nośnik należy poddać testowaniu lub zlikwidować, • opis systemu używanego do tworzenia kopii (w wypadku zmiany systemu, należy zabezpieczyć starszą wersję, do momentu usunięcia kopii stworzonych z wykorzystaniem tego systemu), • procedurę przywracania poszczególnych elementów (plików, systemów, baz danych, itd.), uwzględniającą niezbędne zasoby oraz czas przywrócenia, • procedurę przenoszenia kopii do innych lokalizacji, • procedurę testowania poprawności wykonania kopii, • procedurę okresowych testów polegających na przywróceniu

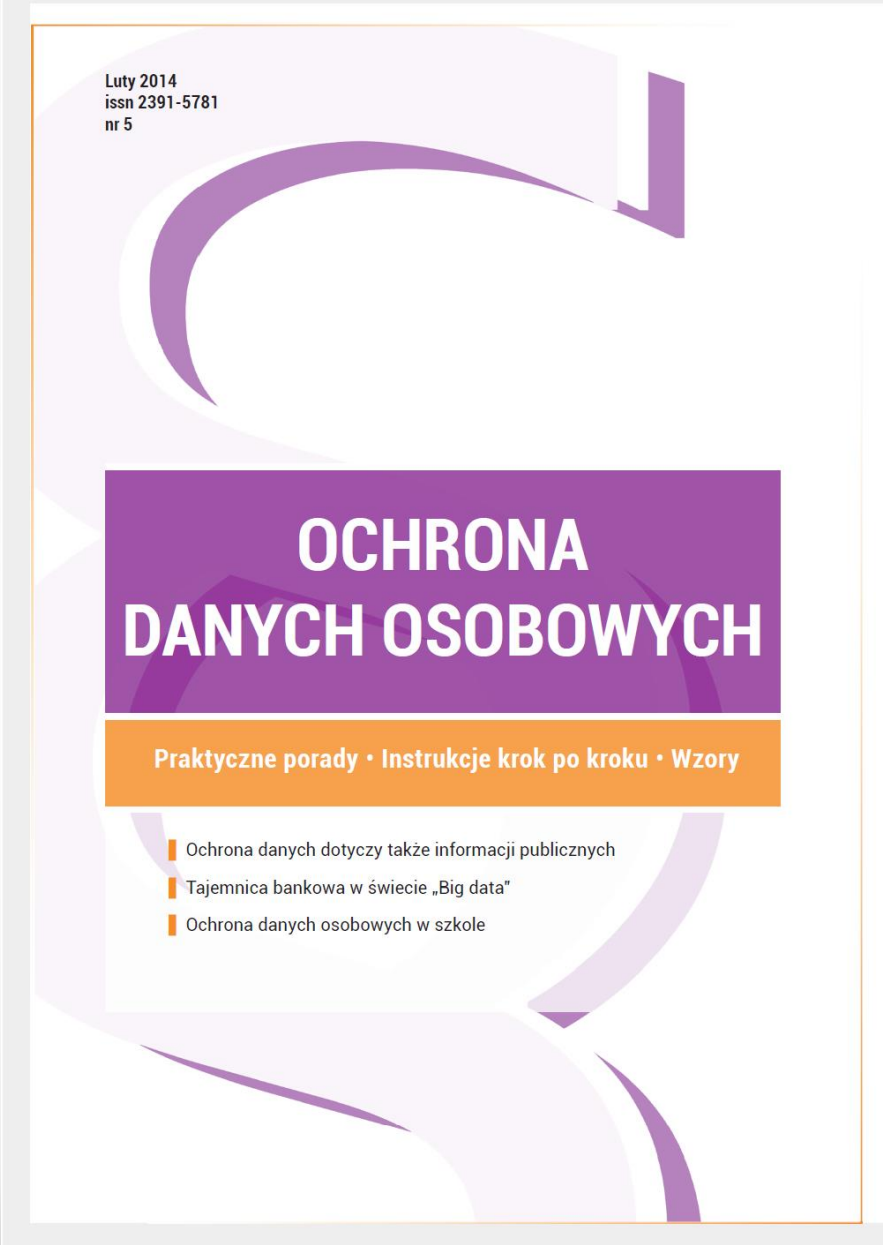
	poszczególnych elementów z kopii, • wskazanie osób odpowiedzialnych za poszczególne czynności, Wybierając rozwiązania techniczne oraz opracowując harmonogram szkoleń powinniśmy brać pod uwagę czy odtwarzając dane zapewnimy utrzymanie wymaganych przez biznes parametrów. W szczególności powinniśmy wziąć pod uwagę czasy RTO i RPO.
5) sposób, miejsce i okres przechowywania: a) elektronicznych nośników informacji zawierających dane osobowe, b) kopii zapasowych, o których mowa w pkt 4,	Należy wskazać miejsce i okres przechowywania poszczególnych nośników, dlatego konieczne jest wprowadzenie pełnej ewidencji wykorzystywanych nośników: • dysków przenośnych, • pendrive, • kart pamięci, • płyt cd/dvd, • smartfonów, • komputerów przenośnych, • taśm streamerów, • wymontowanych dysków, • oraz wszelkich innych nośników wykorzystywanych w organizacji. Musimy zawsze wiedzieć, jakie dane i od kiedy znajdują się na danym nośniku – tyko w ten sposób zagwarantujemy, że spełniona zostanie zasada ograniczenia czasowego. W wypadku kopii zapasowych zaleca się, aby przynajmniej część z nich przechowywana była w innej lokalizacji. Stanowić to będzie zabezpieczenie przed utratą danych na wypadek kradzieży, zalania, pożaru, itd.

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;	Należy wskazać zainstalowane systemy antywirusowe (oraz inne systemy chroniące przed złośliwym oprogramowaniem), w jaki sposób są zarządzane oraz kto odpowiada za ich prawidłowe funkcjonowanie. Należy opisać, w jaki sposób mają postępować użytkownicy oraz administratorzy systemów w razie wykrycia działania złośliwego oprogramowania.
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;	Należy opisać, w jaki sposób odnotowywana jest informacja o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia. Zgodnie z rozporządzeniem, w przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, informacje te mogą być odnotowywane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	Należy stworzyć procedury przeglądów i konserwacji systemów, uwzględniając zakres i częstotliwość przeglądów oraz wskazać osoby odpowiedzialne. Ponieważ urządzenia i nośniki przekazywane do naprawy pozbawia się wcześniej zapisu danych lub naprawia pod nadzorem, należy to uwzględnić w tworzonej procedurze. Stosowanym w praktyce rozwiązaniem jest zawarcie odpowiedniej umowy powierzenia z dostawcą usług serwisowych. Należy także opisać sposób postępowania w wypadku sprzętu objętego gwarancją.

Autor: Jarosław Żabówka

trener, wykładowca, popularyzator zagadnień ochrony danych osobowych, właściciel firmy www.proInfoSec.pl, wieloletni administrator bezpieczeństwa informacji, twórca systemów zarządzania ochroną danych osobowych w małych i dużych przedsiębiorstwach, audytor normy ISO 27001 i manager systemów informatycznych, autor publikacji i prezentacji branżowych

POLECAMY



Działaj zgodnie z prawem!

Stopka redakcyjna

Autor:	Jarosław Żabówka
Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-3785-9
E-book nr:	2HH0337
Wydawnictwo:	Wydawnictwo Wiedza i Praktyka sp. z .o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł