Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

Jednym z wymogów nałożonych na administratorów danych, zgodnie z §3 ust.1 przez rozporządzenie Ministra Spraw Wewnętrznych i Administracji 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. Nr 100 poz. 1024), jest opracowanie instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zwanej dalej „instrukcją".

Opracowana instrukcja powinna być zatwierdzona przez administratora danych i przyjęta do stosowania, jako obowiązujący dokument. Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności. Np. zasady i procedury nadawania uprawnień do przetwarzania danych osobowych, czy też sposób prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych powinny być przekazane osobom zarządzającym organizacją przetwarzania danych, zaś sposób rozpoczęcia i zakończenia pracy, sposób użytkowania systemu, czy też zasady zmiany haseł - wszystkim osobom będącym jego użytkownikami, zasady ochrony antywirusowej, a także procedury wykonywania kopii zapasowych – osobom zajmującym się techniczną eksploatacją i utrzymaniem ciągłości pracy systemu.

W treści instrukcji powinny być zawarte ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, zastosowane rozwiązania techniczne, jak również procedury eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. W przypadku, gdy administrator danych, do przetwarzania danych wykorzystuje nie jeden, lecz kilka systemów informatycznych, wówczas stosownie do podobieństwa zastosowanych rozwiązań powinien opracować jedną, ogólną instrukcję zarządzania lub opracować oddzielne instrukcje dla każdego z użytkowanych systemów. W zależności, zatem od przyjętego rozwiązania, inny będzie zakres opracowanych zagadnień w małych podmiotach, w których dane osobowe przetwarzane są przy pomocy jednego lub kilku komputerów i inny w dużych podmiotach, w których funkcjonują rozbudowane lokalne sieci komputerowe z dużą ilością serwerów i stacji roboczych przetwarzających dane przy użyciu wielu systemów informatycznych.

W instrukcji, o której mowa, powinny być wskazane systemy informatyczne, których ona dotyczy, ich lokalizacje, stosowane metody dostępu (bezpośrednio z komputera, na którym system jest zainstalowany, w lokalnej sieci komputerowej, czy też poprzez sieć telekomunikacyjną np. łącze dzierżawione, Internet). Instrukcja ta powinna obejmować zagadnienia dotyczące zapewnienia bezpieczeństwa informacji, a w szczególności elementy wymienione w §5 rozporządzenia, na które składają się:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt. 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

W celu zapewnienia ochrony przetwarzanych danych, w odniesieniu do każdego z wymienionych wyżej punktów, w treści instrukcji powinny być wskazane odpowiednie dla stosowanych systemów informatycznych zasady postępowania. Ogólne wskazówki dotyczące zagadnień, jakie powinny być zawarte w instrukcji w odniesieniu do wyżej wymienionych punktów przedstawiono poniżej.

1. **Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (§ 5 pkt 1 rozporządzenia)..**

   W punkcie tym powinny zostać opisane zasady przyznawania użytkownikowi identyfikatora w systemie informatycznym, jak również zasady nadawania lub modyfikacji uprawnień użytkownika do zasobów systemu informatycznego. Powyższe zasady powinny obejmować operacje związane z nadawaniem użytkownikom uprawnień do pracy w systemie informatycznym począwszy od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień aż do momentu usunięcia konta z systemu informatycznego. Procedura określająca zasady rejestracji użytkowników powinna w sposób jednoznaczny określać zasady postępowania z hasłami użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych), jak również zasady administrowania systemem informatycznym w przypadkach awaryjnych np. nieobecności administratora.
   W instrukcji należy wskazać osoby odpowiedzialne za realizację procedur oraz rejestrowanie i wyrejestrowywanie użytkowników w systemie informatycznym.

2. **Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem (§ 5 pkt 2 rozporządzenia).**

   W punkcie tym powinien zostać opisany tryb przydzielania haseł, tj. wskazanie, czy hasła użytkowników przekazywane mają być w formie ustnej czy pisemnej oraz wskazanie zaleceń dotyczących stopnia ich złożoności. Powinny zostać również wskazane osoby odpowiedzialne za przydział haseł. Wskazanie to może być określone funkcjonalnie lub personalnie. Zaleca się, aby unikać przekazywania haseł przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. Użytkownik po otrzymaniu hasła powinien być zobowiązany do niezwłocznej jego zmiany, chyba, że system nie umożliwia wykonania takiej operacji. W zależności od stosowanych rozwiązań należy podać dodatkowe informacje dotyczące haseł, takie jak wymogi dotyczące ich powtarzalności czy też wymogi dotyczące zestawu tworzących je znaków. Powinna być również zawarta informacja o wymaganej częstotliwości i metodzie zmiany hasła np. czy zmiana hasła wymuszana jest po określonym czasie przez system informatyczny, czy też użytkownik sam musi o tym pamiętać. Przy określaniu częstotliwości zmiany haseł należy pamiętać, iż zgodnie z pkt IV ppk 2 załącznika do

rozporządzenia, hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 znaków, jeżeli w systemie nie są przetwarzane dane, o których mowa w art. 27 ustawy lub 8 znaków, jeżeli takie dane są przetwarzane (pkt VII załącznika). Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej. Należy wskazać sposób przechowywania haseł użytkowników posiadających uprawnienia administratorów systemów informatycznych oraz sposób odnotowywania ich awaryjnego użycia. Dodatkowo, w przypadku zastosowania innych niż identyfikator i hasło metod weryfikacji tożsamości użytkownika, np. kart mikroprocesorowych czy też metod biometrycznych w instrukcji powinny być zawarte wytyczne w zakresie ich stosowania. Dla kart mikroprocesorowych np. należy wskazać sposób ich personalizacji, zaś dla metod biometrycznych sposób pobierania danych biometrycznych w procesie rejestrowania użytkownika w systemie oraz sposób ich przechowywania.

3. **Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu (§ 5 pkt 3 rozporządzenia).**

   W punkcie tym powinny być wskazane kolejne czynności, jakie należy wykonać w celu uruchamiania systemu informatycznego, a w szczególności zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Przestrzeganie określonych w instrukcji zasad powinno zapewniać zachowanie poufności haseł oraz uniemożliwiać nieuprawnione przetwarzanie danych. Należy również określić metody postępowania w sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w okolicznościach, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba. Użytkownik powinien być poinstruowany o konieczności wykonania operacji wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji komputerowej oraz o czynnościach, jakie w tym celu powinien wykonać. Procedury przeznaczone dla użytkowników systemu powinny wskazywać sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu np. w przypadku braku możliwości zalogowania się użytkownika na jego konto czy też w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe.

4. **Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia).**

   W punkcie tym należy wskazać metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania. Należy określić, dla jakich danych wykonywane będą kopie zapasowe, typ nośników, na których kopie będą wykonywane oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystywane. W procedurze wykonywania kopii powinien być określony harmonogram wykonywania kopii zapasowych dla poszczególnych zbiorów danych wraz ze wskazaniem odpowiedniej metody sporządzania kopii (kopia przyrostowa, kopia całościowa). Fragment instrukcji dotyczący wykonywania kopii zapasowych w przypadku, gdy procedury wykonywania tych kopii są złożone, może się odwoływać do procedur szczegółowych dedykowanych poszczególnym zbiorom danych, czy też systemom informatycznym. Procedury takie powinny być wówczas załączone do instrukcji zarządzania. W procedurach określających zakres i sposób wykonywania kopii zapasowych powinny być wskazane okresy rotacji oraz całkowity czas użytkowania poszczególnych nośników danych. Powinny być określone procedury likwidacji nośników zawierających kopie zapasowe danych po ich wycofaniu na skutek utraty przydatności lub uszkodzenia. Procedura likwidacji nośników zawierających dane osobowe powinna uwzględniać wymogi zawarte w pkt VI ppkt 1 załącznika do rozporządzenia. Wymogi te nakazują, aby urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawiać zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadzać w sposób uniemożliwiający ich odczytanie.

5. **Sposób, miejsce i okres przechowywania:**

   a) **elektronicznych nośników informacji zawierających dane osobowe,**

   b) **kopii zapasowych, o których mowa w §5 pkt. 4 rozporządzenia.**

   W tym punkcie instrukcji należy określić sposób i czas przechowywania wszelkiego rodzaju nośników informacji (dyskietki, płyty CD, taśmy magnetyczne). Należy wskazać pomieszczenia, przeznaczone do przechowywania nośników informacji, jak również sposób zabezpieczenia tych nośników przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.

Przy opracowywaniu zaleceń dotyczących sposobu i czasu przechowywania nośników informacji należy uwzględnić, iż zgodnie z wymogami pkt IV ppkt 4a załącznika do rozporządzenia, kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Należy uwzględnić wymogi określone w pkt IV ppkt 4b załącznika do rozporządzenia nakazujące, aby kopie awaryjne bezzwłocznie usuwać po ustaniu ich użyteczności.

W przypadku przekazywania nośników informacji podmiotom zewnętrznym w celu bezpiecznego ich przechowywania, np. stosowane dość często deponowanie kopii zapasowych w skarbcach bankowych, należy określić procedury przekazywania nośników informacji tym podmiotom oraz wskazać metody zabezpieczania przekazywanych nośników informacji przed dostępem osób nieuprawnionych podczas ich transportu/przekazywania.

6. **Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia).**

W opisie zabezpieczeń systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia należy określić obszary systemu informatycznego narażone na ingerencję wirusów komputerowych oraz wszelkiego rodzaju innego szkodliwe oprogramowanie. Należy wskazać możliwe źródła przedostania się szkodliwego oprogramowania do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość zainstalowania się takiego oprogramowania. Niezależnie od wskazania czynności profilaktycznych przed przedostaniem się do systemu oprogramowania szkodliwego, w instrukcji należy wskazać zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego działania takiego oprogramowania. Należy wskazać oprogramowanie antywirusowe, które zostało zainstalowane, określić metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie tym oprogramowaniem. Powinny być przedstawione również procedury postępowania użytkowników na okoliczność zidentyfikowania określonego typu zagrożeń. Użytkownik powinien być poinformowany o czynnościach, które powinien wykonać w przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia. W przypadku, gdy stosowane są inne niż oprogramowanie antywirusowe metody ochrony przed szkodliwym oprogramowaniem

należy je wskazać i przedstawić procedury związane z ich stosowaniem. Do metod takich mogą należeć m. in. fizyczne odłączenie urządzeń umożliwiających odczyt danych z wymiennych nośników informatycznych poszczególnych stacji komputerowych (np. odłączenie stacji CD, stacji dyskietek, itp.) i wyznaczenie wydzielonego stanowiska w sieci komputerowej do wymiany danych za pomocą nośników zewnętrznych.

7. **Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4.**

Zgodnie z § 7 ust. 1 pkt. 4 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom, w rozumieniu art. 7 pkt. 6 ustawy, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych. Wynika stąd, że system informatyczny wykorzystywany do przetwarzania danych osobowych powinien posiadać funkcjonalności umożliwiające odnotowanie wspomnianych wyżej informacji. Sposób oraz forma odnotowania, jak wynika z § 5 pkt. 7 rozporządzenia, powinna zostać określona w instrukcji. Przy czym szczególną uwagę zwrócić należy na fakt, iż nie jest wystarczające odnotowanie w formie papierowej informacji, o których mowa w § 7 ust. 1 pkt 4, zatem instrukcja nie może przewidywać takiego sposobu realizacji wspomnianego wymogu, gdyż byłoby to niezgodne z przedstawioną w ustawie definicją systemu informatycznego.

Zauważyć należy również, iż w przypadku przetwarzania danych osobowych nie tylko w jednym systemie informatycznym wymagania, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu. Wynika stąd, że odnotowanie informacji o udostępnieniach możliwe jest w jednym systemie tylko wtedy, gdy zbiór danych przetwarzany w dwóch lub więcej systemach dotyczy dokładnie tych samych osób. Przykładem takiej sytuacji jest korzystanie przez wiele aplikacji z tej samej bazy danych. Niedopuszczalne jest natomiast odnotowanie wskazanej informacji wyłącznie w jednym systemie, gdy grupy osób, których dane przetwarzane są w poszczególnych systemach nie są dokładnie tożsame. W sytuacji, gdy zbiór osób, których dane przetwarzane są w jednym systemie różni się od zbioru osób, których dane przetwarzane są w drugim systemie i nie zachodzi relacja zawierania się pomiędzy tymi zbiorami, wówczas konieczne jest odnotowanie informacji o udostępnieniach odrębnie w każdym systemie

obsługującym te zbiory lub ewentualnie w systemie dedykowanym odnotowaniu informacji, o których mowa w § 7 ust. 1 pkt 4.

8. **Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§ 5 pkt 8 rozporządzenia)**

   W punkcie tym należy określić cel, zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego. Należy wskazać podmioty i osoby uprawnione do dokonywania przeglądów i konserwacji systemu informatycznego. Procedury wykonywania czynności konserwacyjnych systemu, w przypadku, gdy czynności te zleca się osobom nie posiadającym upoważnień do przetwarzania danych (np. specjalistom z firm zewnętrznych), powinny określać sposób, w jaki czynności te nadzorowane są przez administratora danych. W przypadku przekazywania do naprawy nośników informatycznych zawierających dane osobowe należy określić sposób usuwania danych osobowych z tych nośników, przed ich przekazaniem. W procedurach dotyczących naprawy sprzętu komputerowego należy uwzględnić wymóg określony w punkcie **V**I ppkt. 3 załącznika do rozporządzenia, który nakazuje, aby urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy, pozbawiać wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawiać je pod nadzorem osoby upoważnionej przez administratora danych.