

>>

Dane przetwarzane bezpiecznie

DANE OSOBOWE | Odpowiedni system przetwarzania danych osobowych ma olbrzymie znaczenie dla prawidłowego funkcjonowania środków bezpieczeństwa. Szczególnie istotne jest tu określenie granic obszaru, na którym przetwarzanie będzie zachodziło.

Tomasz Cygan

Pod pojęciem przetwarzania danych osobowych rozumieć należy – zgodnie z treścią art. 7 pkt 2 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (DzU z 2001 r. nr 101, poz. 926 ze zm., dalej: uodo) – jakiejkolwiek operacje wykonywane na danych osobowych (np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie), a zwłaszcza te, które wykonuje się w systemach informatycznych. Naturalną konsekwencją tej definicji powinno być objęcie obszarem przetwarzania danych osobowych wszystkich miejsc, w których operacje te są wykonywane. Dotyczy to zwłaszcza operacji przeprowadzanych w takim systemie informatycznym, który wykorzystuje sieci bezprzewodowe lub zdalną łączność z serwerem.

Wytyczenie obszaru

Określenie obszaru przetwarzania danych osobowych stanowi jeden z podstawowych obowiązków związanych z wdrażaniem środków organizacyjnych i technicznych służących do przetwarzania danych osobowych. Regulacja zawarta w art. 36 ust. 1 uodo wskazuje bowiem, że zasadniczym obowiązkiem administratora danych jest zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności powinien on zabezpieczyć dane przed ich: udostępnieniem osobom nieupoważnionym,

zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W związku z tym zwrócić należy uwagę, że faktyczny obszar przetwarzania danych osobowych powinien pokrywać się ze stosowanymi zabezpieczeniami.

Prawidłowe wytyczenie obszaru przetwarzania danych osobowych powinno uwzględniać rodzaj danych (dane osobowe „zwykłe” oraz dane osobowe „wrażliwe”), jak również potencjalne zagrożenia. W przypadku danych osobowych przetwarzanych w systemie informatycznym o możliwości wystąpienia zagrożeń decyduje w głównej mierze podłączenie choćby jednego z urządzeń wchodzących w skład systemu informatycznego do sieci publicznej, np. do Internetu. Wniosek taki płynie bezpośrednio z § 6 ust. 4 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 (DzU nr 100, poz. 1024, dalej: rozporządzenie 1024). Przepis ten wskazuje, że wysoki poziom bezpieczeństwa przetwarzanych danych osobowych stosuje się wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.

Pośrednio taki wniosek wypływa także z punktu 15c części E zgłoszenia zbioru

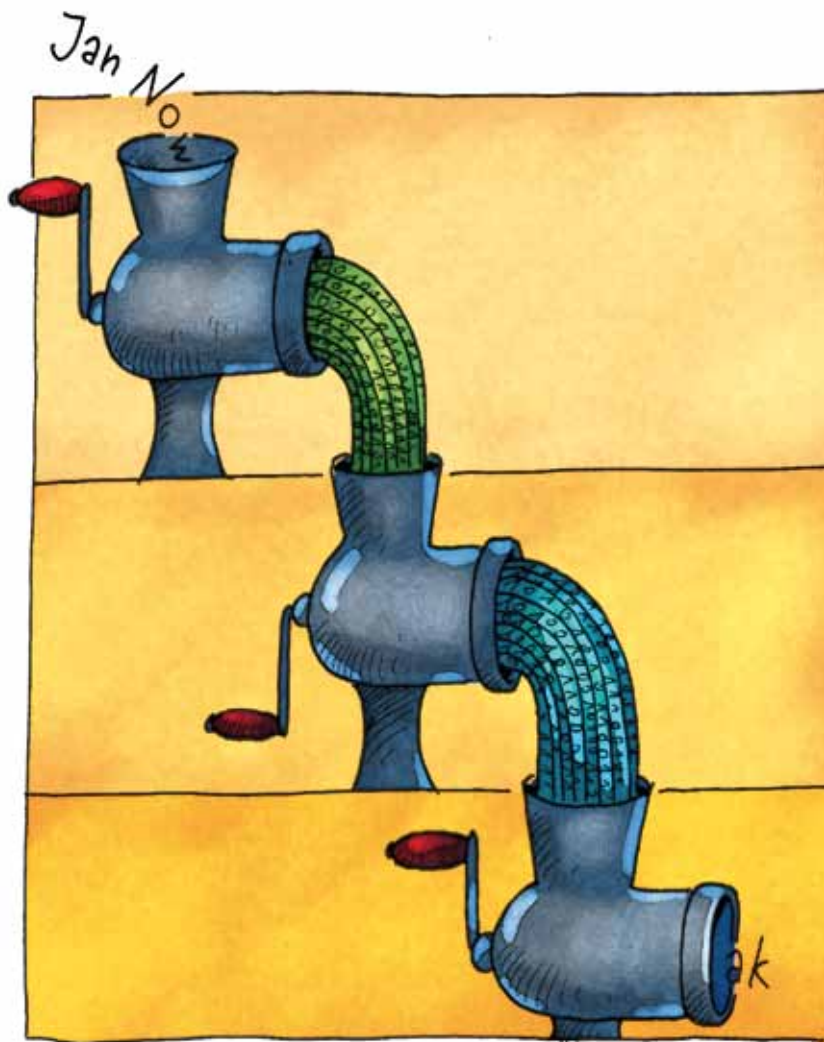
do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych stanowiącego załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (DzU nr 229, poz. 1536). Wskazuje ono Internet jako przykład sieci publicznej skutkującej wdrożeniem wysokiego poziomu bezpieczeństwa.

Polityka zarządzania

Konsekwencją stosowania odpowiednich środków organizacyjnych i technicznych służących ochronie danych osobowych uwzględniających kategorie danych osobowych i występujące zagrożenia jest określony w art. 36 ust. 2 uodo obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz wskazanych powyżej środków. Realizacją tego obowiązku jest § 3 rozporządzenia 1024. Wskazuje on, że w skład takiej dokumentacji wchodzi: polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Natomiast § 4 rozporządzenia 1024, regulując minimalną zawartość polityki bezpieczeństwa, wskazuje, że jednym z jej elementów musi być wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. Przepis, poprzez wyliczenie elementów składających się na obszar przetwarzania danych osobowych, uznać można za swoistą definicję. Nie zawiera ona jednak wszystkich możliwych miejsc, w których wykonywane są operacje na danych osobowych.

Prawidłowe określenie tego obszaru zawierać powinno w pierwszej kolejności dokładne wskazanie miejsca, w którym operacje na danych osobowych są wykonywane. Dlatego też punktem wyjścia musi być podanie danych teleadresowych administratora z uwzględnieniem wszystkich jego lokalizacji. Wynika to z § 4 rozporządzenia 1024, w którym mowa jest o „wykazie budynków” w liczbie mnogiej. Nie wolno przy tym zapomnieć, że miejscem przetwarzania danych osobowych jest także miejsce ich przechowywania.



W związku z tym elementem obszaru przetwarzania danych osobowych są wszelkie archiwa, niezależnie od miejsca ich położenia. Podobnie rzecz ma się z „zewnętrznymi” serwerami (w tym z tymi współdzielonymi z innymi podmiotami) i miejscami przechowywania kopii zapasowych zbiorów danych oraz narzędzi programowych służących do ich przetwarzania. Miejsca przechowywania kopii zapasowych (np. skrytki bankowe) powinny zostać wskazane jako element obszaru przetwarzania danych osobowych.

Kontrola systemu IT

Dobłą praktyką jest precyzyjne wskazanie pomieszczeń obszaru przetwarzania danych osobowych. Sprowadza się to do sprecyzowania, w których konkretnie pomieszczeniach wykonywane są operacje na danych osobowych. Wynika to w głównej mierze z charakteru polityki bezpieczeństwa. Biorąc pod uwagę,

że odgrywa ona także rolę inwentaryzacyjną, precyzyjne wskazanie pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych w sposób znaczący ułatwi dobranie stosownych środków organizacyjnych i technicznych chroniących dane osobowe. Nie wolno przy tym zapominać o specyfice przetwarzania danych osobowych przy użyciu systemu informatycznego. Polityka bezpieczeństwa powinna więc uwzględniać wszelkie elementy wchodzące w skład takiego systemu informatycznego.

Zgodnie z treścią art. 7 pkt 2a uodo system informatyczny jest zespołem współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Uznać należy, że jeżeli poszczególne elementy systemu informatycznego biorą udział w przetwarzaniu danych osobowych, to miejsca, w których one się znajdują, powinny zostać >>

» sprecyzowane w polityce bezpieczeństwa. Warto przy tym pamiętać o miejscach, w których przechowywane są nośniki informacji – także te uszkodzone i przeznaczone do likwidacji oraz uszkodzone stacje robocze zawierające dane osobowe. W związku z tym administrator danych powinien rozważyć prawidłowość sposobu postępowania z takimi nośnikami. Niejednokrotnie bowiem zdarza się, że nośniki (zwłaszcza dyskietki, które wyszły już z użycia) znajdują się na stanie organizacji, ale z powodu braku opisu nikt nie wie, co się na nich znajduje. Wydaje się jednak, że w przeszłość odeszła niechlubna praktyka składowania uszkodzonego sprzętu komputerowego na korytarzach.

Ostrożna praca zdalna

Szczególnego rozważenia wymaga wpływ posiadania komputerów przenośnych na granice obszaru przetwarzania danych osobowych, a także wykorzystywanie ich w pracy „na odległość”. Przepisy rozporządzenia 1024 zawierają w swojej treści pewną wskazówkę na ten temat. Zgodnie z treścią punktu V załącznika A do tego rozporządzenia osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, a także stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

Ponieważ praca jest niejednokrotnie wykonywana poza siedzibą organizacji, można postawić pytanie, czy także te miejsca powinny być uwzględniane jako obszar przetwarzania danych osobowych. Konsekwencją takiego postępowania byłoby jednak rozciągnięcie obszaru na wszystkie miejsca, w których dane osobowe są przetwarzane. Jednocześnie niemożliwe byłoby ustalenie granic takiego obszaru. Wyobraźmy sobie bowiem, że ochrona danych osobowych rozciąga się także na mieszkania pracowników czy też na hotele, w których przebywają w delegacjach służbowych. Wydaje się, że takie podejście do wyznaczania obszaru przetwarzania danych osobowych jest niecelowe i kuriozalne. Również wskazany powyżej punkt V załącznika

A do rozporządzenia 1024 dostarcza argumentów – tym razem prawnych – przeciwko takiemu spojrzeniu. Posługuje się on bowiem konstrukcją „użytkowania” komputera przenośnego poza obszarem przetwarzania danych osobowych. W związku z tym uznać należy, że już sam prawodawca wyłącza miejsca przetwarzania danych osobowych „na odległość” z obszaru przetwarzania danych osobowych. Pozwala to na przyjęcie, że określenie zasad takiego użytkowania w swoisty sposób dopełnia omawiane pojęcie. Dopiero prawidłowe wskazanie obszaru przetwarzania danych osobowych uzupełnione o stosowane zasady użytkowania komputerów przenośnych poza jego obszarem pozwala w sposób pełny spojrzeć na rzeczywiste granice, w których wykonywane są operacje na danych osobowych.

Zasada czystego biurka

Definicja przetwarzania danych osobowych zawarta w art. 7 pkt 2 uodo wskazuje na pierwszorzędą rolę systemów informatycznych w tym procesie. Dlatego też stale na uwadze trzeba mieć sytuację, w której Internet używany w organizacji wykorzystuje sieci bezprzewodowe. W takim przypadku granice fizyczne budynku nie muszą się pokrywać z faktycznym zasięgiem Sieci. Truizmem byłoby zwracanie uwagi na zabezpieczenie sieci bezprzewodowej choćby poprzez stosowanie odpowiednich środków uwierzytelnienia dostępu do niej. Niemniej może się zdarzyć sytuacja, w której spoza fizycznych granic obszaru przetwarzania danych osobowych możliwy będzie dostęp do wszystkich zasobów systemu informatycznego przeznaczonego do przetwarzania danych osobowych.

Ustawodawca wskazuje, że uodo stosuje się do przetwarzania danych w: systemach informatycznych (również w przypadku przetwarzania danych poza zbiorem danych), kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych (art. 2 ust. 2 uodo). Prawidłowe ustalenie obszaru przetwarzania danych osobowych w odniesieniu do zbiorów danych prowadzonych w formie tradycyjnej obejmować będzie miejsca, w których wykonywane są jakiegokolwiek operacje na danych osobowych. Nie

ulega przy tym wątpliwości, że oprócz sytuacji, w których dane osobowe są wykorzystywane „roboczo”, zbiory danych osobowych w wersji papierowej muszą być gdzieś przechowywane. Zajmują one jednak znacznie więcej miejsca od danych posiadających postać elektroniczną. Dlatego opisując obszar, w którym przetwarzane są dane osobowe, należy wziąć pod uwagę miejsce ich składowania, a więc wszelkie pomieszczenia lub ich części, w których znajdują się np. szafy zawierające dokumentację papierową. Dotyczy to również archiwów dokumentów papierowych. Warto przy tym zauważyć, że konsekwencją określenia obszaru przetwarzania danych osobowych posiadających postać papierową będzie zastosowanie zasady „czystego biurka” i obowiązek niszczenia dokumentów papierowych.

Kontrola dostępu

Przepisy prawa oprócz ogólnego wskazania obszaru, w którym przetwarzane są dane osobowe (a więc budynków, pomieszczeń lub części pomieszczeń) nie zawierają żadnych szczególnych wskazań co do sposobów jego zabezpieczenia. Jedynym wyjątkiem jest regulacja zawarta w punkcie I załącznika A do rozporządzenia 1024. Zgodnie z jego treścią obszar zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Innymi słowy, przepis ten wskazuje na konieczność rozważenia kontroli dostępu do obszaru. Z treści rozporządzenia wynika też wprost, że upoważnienie do przetwarzania danych osobowych stanowi „przepustkę” wstępu do obszaru, w którym przetwarzane są dane osobowe. Nie oznacza to jednak dostępu bezwarunkowego. Wydaje się bowiem, że dostęp powinien być uzależniony od zakresu danych osobowych przetwarzanych przez określoną osobę. Co więcej, w ramach każdego obszaru przetwarzania danych osobowych wskazać można pomieszczenia, do których dostęp powinien być ściśle limitowany. Przykładem takiego pomieszczenia jest serwerownia. Samo upoważnienie do przetwarzania danych osobowych nie jest przecież równoznaczne z dostępem do serwerów. Na podobnych

zasadach powinien być ograniczony dostęp do pomieszczeń, w których przechowywane są kopie zapasowe zbiorów danych osobowych oraz narzędzi programowych służących do ich przetwarzania.

Inną sytuacją jest możliwość przebywania w obszarze przetwarzania danych osobowych osób nieuprawnionych. Dotyczy to wszystkich klientów organizacji, także osób nieposiadających upoważnień do przetwarzania danych osobowych. Zgodnie z punktem I.2 załącznika A do rozporządzenia 1024 przebywanie osób nieuprawnionych w obszarze jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Warto pamiętać, że niejednokrotnie potrzeby organizacji mogą rozszerzyć zakres osób przebywających w obszarze, np. o personel sprząający. W takim przypadku nadanie uprawnień do przebywania w obszarze przetwarzania danych osobowych w połączeniu ze stosowaniem środków technicznych w postaci szaf zamykanych na klucz oraz środków o charakterze organizacyjnym (takich jak zasada „czystego biurka” czy obowiązek niszczenia dokumentów) może stanowić wystarczające zabezpieczenie obszaru, w którym przetwarzane są dane osobowe.

Znać zasoby

Na pierwszy rzut oka wydawać się może, że wyznaczenie granic obszaru przetwarzania danych osobowych nie stanowi większego problemu. Niemniej do prawidłowego wykonania tego zadania niezbędna jest szczegółowa znajomość własnych zasobów. Brak wystarczającej wiedzy może sprawić, że poza zakresem ochrony pozostaną aktywa ważne dla organizacji. Sytuacja taka najczęściej dotyczy wszelkich niestandardowych miejsc przetwarzania danych osobowych i granic sieci bezprzewodowych stosowanych do przetwarzania danych osobowych.

Autor specjalizuje się w zagadnieniach bezpieczeństwa informacji, ochrony danych osobowych i własności intelektualnej oraz prawa autorskiego. Jest autorem wielu publikacji z tych dziedzin, wykładawcą i konsultantem.

Adwokat, ukończył studia doktoranckie na Wydziale Prawa i Administracji Uniwersytetu Śląskiego w Katowicach.

Komentarz

Polityka bezpieczeństwa danych osobowych



dr Wojciech Rafał Wiewiórowski
Generalny Inspektor Ochrony Danych Osobowych

Przepisy mówią, że obszar przetwarzania danych osobowych powinien zostać określony w polityce bezpieczeństwa. Powinien w niej zostać umieszczony wykaz wszystkich budynków, pomieszczeń i części pomieszczeń, w których dokonywane są wszelkie operacje na danych osobowych, a więc zarówno te dotyczące ich pozyskiwania, opracowywania i modyfikacji, jak i przechowywania, a nawet usuwania. Wykaz powinien zawierać także listę lokalizacji przetwarzania danych w postaci elektronicznej, takich jak serwerownia oraz pomieszczenia, w których znajdują się komputerowe stacje robocze.

Oczywiście, dane osobowe mogą być również przetwarzane poza obszarem opisanym w polityce bezpieczeństwa. Dotyczy to w szczególności sytuacji użytkowania poza tym obszarem komputerów (urządzeń) przenośnych oraz wykonywania tzw. pracy zdalnej. Jeżeli przetwarzanie danych odbywa się przy użyciu wskazanych urządzeń (czyli w różnych miejscach, których nie sposób wymienić), to w polityce bezpieczeństwa powinna znaleźć się informacja jedynie o użytkowaniu takich urządzeń, a tym samym o przetwarzaniu danych poza obszarem. Jednocześnie należy spełnić wymóg zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania komputera przenośnego zawierającego dane osobowe poprzez zastosowanie środków ochrony kryptograficznej wobec przetwarzanych danych osobowych. Ponadto urządzenia i nośniki zawierające tzw. dane wrażliwe (np. o stanie zdrowia, nałogach, pochodzeniu rasowym, przynależności wyznaniowej i życiu seksualnym) przekazywane poza obszar przetwarzania danych osobowych

zabezpiecza się w sposób zapewniający poufność i integralność tych danych. Poufność rozumiana jest jako właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom, zaś integralność – jako właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

W polityce bezpieczeństwa należy zawrzeć również informację o przetwarzaniu danych w związku ze zlecaniem pracy wykonywanej poza obszarem, o którym mowa powyżej, czyli pracy zdalnej. Ze względu na specyfikę przetwarzania danych przez osobę (pracownika, zleceniobiorcę) wykonującą pracę zdalną oczywiste jest, że operacje na danych są wykonywane w miejscu nienależącym do obszaru przetwarzania opisanego w polityce bezpieczeństwa. Przestrzeń przetwarzania danych stanowi zazwyczaj mieszkanie ww. osoby lub inne wybrane przez nią miejsce. Z tego względu administrator danych nie zawsze może w omawianym dokumencie umieścić szczegółowe informacje o miejscu przetwarzania danych. Powinien jednak wskazać, że do takiego przetwarzania danych dochodzi i na jakich zasadach to się odbywa. Ponadto umowa z osobą przetwarzającą dane na zasadzie pracy zdalnej (zleceniodawcą) powinna zawierać postanowienia odnoszące się do zabezpieczenia tych danych, a w szczególności do postępowania podczas transportu, przechowywania i użytkowania komputera przenośnego. Wskazane kwestie powinny zostać także uwzględnione w przeznaczonych dla pracowników wewnętrznych procedurach wdrożonych u pracodawcy zatrudniającego osoby wykonujące wspomniany rodzaj pracy.