DANE OSOBOWE

OCHRONA BAZ DANYCH

Bazy danych są strategicznym zasobem każdej firmy. Równocześnie gromadzone i przetwarzane informacje są cennym łupem dla różnego rodzaju przestępców. Dlatego ważne jest, aby osoby odpowiedzialne za ochronę zbiorów informacji znały przepisy dotyczące zasad korzystania z baz danych oraz elementów ich ochrony.

Dariusz Łydziński

W każdej firmie bazy danych są, zaraz po pracownikach, drugim najcenniejszym zasobem w organizacji. Wszystkie firmy zobowiązane są też poprzez odpowiednie przepisy prawne do ochrony danych dotyczących własnego personelu oraz klientów. Niezależnie od profilu działalności jednostki powinny zostać zastosowane możliwie maksymalne zabezpieczenia oraz dołożona należyta staranność przy obchodzeniu się z gromadzonymi informacjami.

W świetle polskiego prawa bazy danych chronione są na podstawie przepisów zawartych w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (dalej pr.aut.) oraz regulacjach ustawy z dnia 27 lipca 2001 r. o ochronie baz danych (uobd). Ustawa o prawie autorskim znajduje zastosowanie do baz, których dobór, układ i zestawienie ma charakter twórczy. Pozbawia to możliwości objęcia ochroną zbiorów, w których elementy zostały ułożone alfabetycznie czy też chronologicznie. Z uwagi na to ograniczenie uzupełnieniem są przepisy wspomnianej ustawy o ochronie baz danych pozwalające na ochronę zbiorów, które nie spełniają przesłanek umożliwiających uznanie ich za przedmiot prawa autorskiego.

Z uwagi na złożoność tematu, różnorodność podejmowanych przez przedsiębiorców działań oraz zakres stosowanych środków ochrony informacje zawarte w artykule dotyczą tylko jednego z najpopularniejszych zagadnień, a mianowicie ochrony baz danych osobowych.

> BAZY DANYCH OSOBOWYCH – WYMAGANIA PRAWNE

W przypadku większości firm przedmiotem ochrony są bazy niespełniające cech utworu. Należy przy tym zaznaczyć, że za bazę danych uznawany jest zbiór danych lub innych elementów zgromadzony według określonej systematyki lub metody. Jest to ważne, gdyż z punktu widzenia prawa nie ma znaczenia sposób sporządzenia i utrwalenia zbioru. Ustawa o ochronie baz danych dotyczy zbiorów przechowywanych w dowolny sposób. Chronione są więc nie tylko elektroniczne bazy danych, ale również ich wersje papierowe.

WARTO PAMIĘTAĆ

Nawet zwykły katalog może zostać zakwalifikowany jako baza danych i z tego powodu podlegać ochronie prawnej. Nielegalne korzystanie z bazy danych może pociągnąć za sobą odpowiedzialność cywilnoprawną, a nawet karnoprawną.

Ustawa uodb chroni interesy producenta bazy, którym może być osoba fizyczna, osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej ponosząca nakłady inwestycyjne na tworzenie bazy. Producentem bazy powstałej w wyniku stosunku pracy jest pracodawca. Producentem bazy powstałej na podstawie umowy o dzieło lub zlecenie jest zleceniodawca. Ustawa ta określa także czas obowiązywania ochrony bazy danych, który wynosi 15 lat od momentu jej utworzenia lub od momentu jej udostępnienia publicznie, o ile nastąpiło w ciągu 15 lat od jej utworzenia.

Ustawodawca docenił rolę tych, którzy zbierają informacje, gromadzą je i przetwarzają lub udostępniają przetwarzanie dla określonych osób i celów. W przypadku bezprawnego korzystania z chronionej bazy danych producent ma prawo wezwać do zaprzestania korzystania (uobd art. 11) z bazy, zwrotu uzyskanych korzyści finansowych lub żądać naprawienia wyrządzonej szkody na prawach ogólnych. Osoba korzystająca z chronionej bazy danych podlega karze grzywny.

> OCHRONA DANYCH OSOBOWYCH

Zasady przetwarzania danych osobowych w zbiorach danych, a za takie możemy uznać bazy danych osobowych, określa ustawa z dnia 29 sierpnia +

1997 r. o ochronie danych osobowych (dalej uodo) oraz wydane na jej podstawie akty wykonawcze – rozporządzenia 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.

Ustawa (uodo) określa zasady postępowania przy przetwarzaniu tego typu danych oraz prawa osób, których dane są przetwarzane, niezależnie od sposobu ich przetwarzania. Ustawa nakłada również na administratorów baz danych osobowych konkretne wymagania organizacyjne i techniczne. W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji ustawa definiuje następujące kwestie:

- określenie pojęcia danych osobowych (art. 6 uodo);
- określenie zasad przetwarzania danych osobowych (rozdz. 3 uodo);
- wskazanie praw osoby, której dane są przetwarzane (rozdz. 4 uodo);
- aspekty zabezpieczania danych osobowych (rozdz. 5 uodo);
- obowiązek rejestrowania zbiorów danych osobowych (rozdz. 6 uodo);
- zasady przekazywania danych osobowych do państwa trzecich (rozdz. 7 uodo);
- określenie organów ochrony danych osobowych, w tym wyszczególnienie praw i obowiązków Generalnego Inspektora Ochrony Danych Osobowych i obowiązków podmiotów względem GIODO.

> ZABEZPIECZANIE DANYCH OSOBOWYCH

Zasady zabezpieczenia baz danych osobowych zarówno w sposób techniczny, jak i organizacyjny zawiera rozdz. 5 uodo. Wymagania dotyczące zabezpieczeń danych osobowych najogólniej określa art. 36 ust. 1 uodo, w którym napisano, że „administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem”.

Artykuł 39a uodo określa, że podstawowe warunki organizacyjne i techniczne, jakie muszą spełniać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, są wskazane w rozporządzeniu MSWiA 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”. **Rozporządzenie to jest podstawowym dokumentem określającym wymagania techniczne dotyczące systemów informatycznych**. W załączniku do tego rozporządzenia wymienione są środki bezpieczeństwa, jakie powinny być stosowane w systemie informatycznym przetwarzającym dane osobowe. Zostały one przypisane do trzech poziomów zabezpieczeń:

- podstawowy – dla wszystkich systemów;
- podwyższony – dla systemów przetwarzających dane o szczególnej wartości wymienione w art. 27 uodo (tzw. dane wrażliwe);
- wysoki – gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.

Dużą rolę w zakresie bezpieczeństwa i zasad korzystania z baz danych osobowych odgrywa, oprócz wspomnianych już aspektów, element rozliczalności. Podkreślając globalny charakter przepisów o ochronie danych osobowych,

WYMAGANIA DOTYCZĄCE OCHRONY BAZ DANYCH

Najważniejsze wymagania dotyczące ochrony baz danych osobowych wynikające z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych to:

- Określenie aspektów identyfikacji, czy w administrowanej bazie danych znajdują się dane osobowe.
- Określenie zakresu przetwarzania administrowanych danych, identyfikacja, czy jest wymagana i dostępna zgoda osób, których dane dotyczą, weryfikacja kompletności danych i poprawności ich przetwarzania ze zgłoszonym celem i zakresem.
- Określenie mechanizmów udostępniania danych i weryfikacja rejestracji udostępniania danych. Baza danych osobowych powinna umożliwiać wyświetlenie i wydrukowanie dla danej osoby raportu, w którym będą uwzględnione: dane osoby, źródło pochodzenia danych, kto dopisał dane do bazy, data i czas utworzenia wpisu, informacje o modyfikacjach, informacje, komu, kiedy i w jakim zakresie dane były udostępniane.
- Określenie formatu przekazywania danych, zakresu i rejestrowania przekazywania danych.
- Określenie poziomu bezpieczeństwa dla każdego ze zbiorów, nadawanie i zarządzanie upoważnieniami do przetwarzania danych osobowych oraz stosowania mechanizmów rozliczalności.
- Sporządzenie dokumentacji dotyczącej sposobu przetwarzania i zabezpieczania danych osobowych.
- Określenie zasad kontroli i dostępu do obszarów przetwarzania danych osobowych.
- Określenie fizycznych zabezpieczeń instalacji informatycznych, baz danych i nośników zawierających dane osobowe.
- Wyznaczenie osób odpowiedzialnych za fizyczne bezpieczeństwo instalacji informatycznych, baz danych i nośników zawierających dane osobowe.
- Określenie sposobu weryfikowania nadanych uprawnień dostępu do systemów.

WYMAGANIA DOTYCZĄCE SYSTEMÓW IT

Najważniejsze wymagania określone w rozporządzeniu MSWiA z dnia 29 kwietnia 2004 r. dotyczące urządzeń i systemów informatycznych służących do przetwarzania danych osobowych:

- Konieczność stosowania mechanizmów kontroli dostępu, przy czym jeśli do systemu ma dostęp wielu użytkowników, muszą mieć oni odrębne identyfikatory. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
- Zabezpieczenie przed „działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego" oraz „utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej".
- Konieczność sporządzania kopii zapasowych danych i programów je przetwarzających, przy czym kopie zapasowe należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwać niezwłocznie po ustaniu ich użyteczności.
- Konieczność szyfrowania danych przetwarzanych na komputerze przenośnym.
- Obowiązek usunięcia zapisanych danych w sposób uniemożliwiający ich odzyskanie z dysków lub innych nośników elektronicznych zawierających dane osobowe, przeznaczonych do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do przetwarzania danych osobowych.
- Konieczność stosowania na poziomie wysokim zabezpieczeń logicznych, które obejmują kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań z sieci publicznej i systemu informatycznego administratora danych.
- Konieczność zapewnienia na poziomie wysokim ochrony kryptograficznej danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.
- Hasło powinno składać się co najmniej z sześciu znaków na poziomie podstawowym, a na poziomie podwyższonym i wysokim z ośmiu znaków, i zawierać małe i duże litery oraz cyfry lub znaki specjalne. Hasła powinny być zmieniane nie rzadziej niż co 30 dni.

należy wspomnieć §7 rozporządzenia 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. W dokumencie zostały ujęte główne wytyczne w tym zakresie:

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych ma wyłącznie jedna osoba;
3) źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą;
4) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

W świetle przytoczonego ust. 1 pkt 1 i 2 widać, że w systemie informatycznym konieczne jest istnienie indywidualnego autoryzowanego dostępu dla każdego użytkownika oraz rejestracja czasu zdarzeń wygenerowanych przez niego samego. Powiązanie tych faktów z wymogiem odnotowywania identyfikatora użytkownika wprowadzającego dane (wraz z datą pierwszego wprowadzenia danych) oraz automatyzacją tych procesów (zgodnie z §7 ust. 2) daje w konsekwencji brak możliwości istnienia anonimowych działań użytkowników.

Odpowiedzialność użytkowników, jak również świadomość rejestrowania przez system wszystkich ich działań, zazwyczaj zapobiega zjawisku udostępniania haseł i identyfikatorów. Bezpośrednio zwiększa to bezpieczeństwo przetwarzania danych w bazach danych osobowych.

Z kolei ust. 1 pkt 3, 4 i 5 dotyczą bezpieczeństwa osób, których dane osobowe są przetwarzane. Źródło pochodzenia informacji przechowywanych w bazie, a także zapisy, komu, kiedy i w jakim zakresie dane zostały udostępnione, oraz możliwość zgłoszenia i odnotowania sprzeciwu dotyczącego przetwarzania danych osobowych sprawiają, że każda osoba, której dane są przetwarzane, może kontrolować sposób przetwarzania danych o sobie.

> ZASADY KORZYSTANIA Z BAZ DANYCH OSOBOWYCH

Zbiory gromadzonych danych osobowych powinny być zabezpieczone przed dostępem osób nieuprawnionych i stanowić odrębną bazę danych w każdej organizacji. Przekazywanie danych osobowych osobom trzecim oraz instytucjom +

ZASADA DOZWOLONEGO UŻYTKU

Ustawa o ochronie baz danych pozwala na korzystanie z baz danych na zasadzie tzw. dozwolonego użytku. Zgodnie z art. 8 uobd możliwe jest korzystanie z istotnej co do jakości lub ilości części rozpowszechnionej bazy danych:

- do użytku osobistego, ale tylko z zawartości nieelektronicznej bazy danych;
- w charakterze ilustracji, w celach dydaktycznych lub badawczych, ze wskazaniem źródła, jeżeli takie korzystanie jest uzasadnione niekomercyjnym celem, dla którego wykorzystano bazę;
- do celów bezpieczeństwa wewnętrznego, postępowania sądowego lub administracyjnego.

jest dozwolone za zgodą osoby, której dane dotyczą, oraz gdy wymagają tego obowiązujące przepisy prawa. Korzystanie z baz danych osobowych związane jest z procesami udostępniania danych oraz powierzania baz danych do przetwarzania.

UDOSTĘPNIANIE DANYCH OSOBOWYCH – następuje wtedy, gdy administrator danych osobowych przekaże w sposób faktyczny lub umożliwi w inny sposób zapoznanie się z danymi osobie trzeciej lub podmiotowi, który pełnić będzie w stosunku do tych danych osobowych rolę administratora danych.

Procesy związane z udostępnianiem danych z baz danych osobowych dzielą się na udostępnianie danych wewnątrz i na zewnątrz organizacji. Przy udostępnianiu danych wewnątrz organizacji należy zwrócić uwagę, aby dane udostępniać jedynie osobom mającym upoważnienie do przetwarzania danych osobowych, którym dane te są potrzebne do wykonywania ich obowiązków służbowych. Udostępniając dane na zewnątrz organizacji, należy upewnić się, czy istnieje podstawa prawna udostępnienia danych osobowych. Dane powinno się udostępniać innym podmiotom na podstawie pisemnego wniosku, w którym powołano się na przepisy zezwalające na udostępnienie danych.

POWIERZENIE DANYCH DO PRZETWARZANIA – wiąże się z procesami zlecania czynności przetwarzania danych osobowych innym podmiotom. Zlecenie tego typu czynności w imieniu danej organizacji musi odbywać się na podstawie umowy pisemnej. Aby przekazanie danych było w pełni legalne, konieczne jest zawarcie stosownej umowy powierzenia.

Zasady zawierania umów powierzenia określa szczegółowo art. 31 ustawy o ochronie danych osobowych. Zgodnie z tym artykułem administrator danych powinien określić środki i cele przetwarzania danych przez zleceniobiorcę, który może wykorzystywać dane wyłącznie w sposób określony w zawartej umowie powierzenia. Podmiot, który pozyskuje w taki sposób dane, nie ma więc statusu administratora i nie może z nich dowolnie korzystać (zakaz wykorzystania danych osobowych dla własnych celów).

Podmiot, któremu powierza się dane osobowe do przetwarzania, zobowiązuje się w umowie do przetwarzania danych jedynie w opisanym celu i zakresie, jak również do zastosowania środków zabezpieczających, o których mowa w art. 36–39 uodo. Równocześnie podmiot ten nie jest zobowiązany do realizacji obowiązków określonych w ustawie o ochronie danych osobowych (m.in. nie musi zgłaszać do rejestracji zbioru danych osobowych). Z kolei administrator danych zobowiązany jest do wykonywania wszystkich obowiązków określonych w przepisach o ochronie danych osobowych, w tym m.in. musi zgłosić zbiór danych osobowych do rejestracji GIODO i ponosi odpowiedzialność administracyjną za naruszenie przepisów o ochronie danych osobowych.

Obydwa podmioty są zobowiązane do przestrzegania przepisów rozporządzenia wykonawczego do ustawy o ochronie danych osobowych, regulującego kwestie zabezpieczenia danych. W tym zakresie ponoszą pełną odpowiedzialność zarówno administracyjną, jak i karną wynikającą z przepisów ustawy.

> WARTOŚĆ DLA FIRMY

Bazy danych osobowych obejmują dane, które mają wymierną wartość dla firm. Nie dziwi więc, że trudno znaleźć przedsiębiorstwo skore do współdzielenia tego typu informacji z konkurencją.

Ważnymi elementami wynikającymi z dobrych praktyk, na które nacisk kładą akty prawne związane z ochroną baz danych osobowych, są:

- bezpieczeństwo fizyczne danych osobowych przetwarzanych elektronicznie i tradycyjnie,
- bezpieczeństwo systemów informatycznych, służących do przetwarzania danych osobowych,
- bezpieczeństwo danych osobowych w oparciu o środki organizacyjne.

Ustawa o ochronie danych osobowych stanowi w art. 1, że każdy ma prawo do ochrony dotyczących go danych osobowych, a przetwarzanie danych osobowych powinno uwzględniać dobro publiczne, dobro osoby, której dane dotyczą, oraz dobro osób trzecich w zakresie i trybie określonym ustawą. Oznacza to generalny zakaz przetwarzania danych osobowych bez uzasadnienia i wymóg ustawowego regulowania zakresu i trybu przetwarzania danych osobowych.

Autor jest szefem działu bezpieczeństwa, ochrony informacji i audytu w dużej firmie informatycznej. Prowadzi szkolenia dotyczące ochrony danych osobowych, polityki bezpieczeństwa oraz bezpieczeństwa IT. Specjalizuje się w technologiach związanych z infrastrukturą klucza publicznego oraz rozwiązaniach e-security. Trener i koordynator projektów, audytor systemów zarządzania bezpieczeństwem informacji.