

Wymagania dotyczące bezpieczeństwa informacji i baz danych zawarte w obowiązujących w Polsce aktach prawnych

Jakub Radziulis, prof. Witold Hołubowicz

Uniwersytet im. Adama Mickiewicza w Poznaniu
e-mail: radziuli@amu.edu.pl, holub@amu.edu.pl

Rafał Knapik

ITTI Sp. z o.o.
e-mail: rafal.knapik@itti.com.pl

Abstrakt

Artykuł dokonuje analizy obowiązujących w Polsce aktów prawnych pod kątem zapisów dotyczących zabezpieczeń baz danych i informacji przechowywanych w tych bazach. Analiza jest przeprowadzona w celu określenia, na jakie przepisy prawa musi wrócić uwagę administrator bazy danych oraz właściciel danych w zależności od informacji jaka jest w niej przechowywana i charakterystyki organizacji, która wykorzystuje daną bazę (podmiot publiczny, czy podmiot prywatny). W ramach artykułu przedstawione zostały wymagania dotyczące bezpieczeństwa zawarte m.in. w ustawie o ochronie danych osobowych, ustawie o ochronie baz danych, ustawie o informatyzacji działalności podmiotów publicznych, ustawie o świadczeniu usług drogą elektroniczną, ustawie o ochronie informacji niejawnych, ustawie skarbowej, prawie telekomunikacyjnym oraz powiązanych z tymi ustawami rozporządzeniach. W artykule zwrócona została uwaga na aspekty związane z odpowiedzialnością właściciela bazy danych za informację w niej przechowywaną i przedstawione zostały sytuacje, w których jest on z tej odpowiedzialności zwolniony.

Wstęp

Punktem wyjścia do przeprowadzenia analizy aktów prawnych pod kątem stawianych przez nie wymagań bezpieczeństwa dla baz danych i informacji w nich przechowywanych było powszechnie wykorzystywane stwierdzenie: „Nieznajomość prawa nie zwalnia z odpowiedzialności za jego przestrzeganie”.

Mnogość aktów prawnych, które definiują i określają zasady postępowania w zakresie ochrony informacji w zależności od jej rodzaju, może spowodować sytuację, w której użytkownik nie jest świadomy, że podejmowane przez niego działania mogą podlegać regulacjom prawnym. Zapewne nikt nie chce, przynajmniej świadomie, nie przestrzegać obowiązującego w Polsce prawa. Zgodność z regulacjami prawnymi powinna być dla każdego podmiotu priorytetem, czy to w działaniu biznesowym czy też w innym. Zgodność ta ma wpływ na pozycję i konkurencyjność podmiotów biznesowych oraz na prawidłowe wykonywanie statutowych działań w przypadku instytucji publicznych. Zatem znajomość i stosowanie regulacji prawa dotyczących bezpieczeństwa baz danych i informacji w nich zawartych jest kwestią istotną dla każdego administratora baz danych. Świadomość, które akty prawne dotyczą ich działania, oraz które zapisy są w nich najważniejsze, zdaje się być dla administratorów elementem koniecznym w ich codziennej pracy. Mamy nadzieję, że po przeczytaniu niniejszego artykułu wiedza w wymienionym zakresie zostanie poszerzona.

W niniejszym artykule analizie zostały poddane następujące ustawy i rozporządzenia odnoszące się do baz danych lub informacji w nich przechowywanych:

- Ustawa o ochronie danych osobowych,
- Ustawa o ochronie baz danych,
- Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne,
- Ustawa o świadczeniu usług drogą elektroniczną,
- Ustawa o ochronie informacji niejawnych,
- Ustawie o rachunkowości,
- Prawo Telekomunikacyjne,
- Rozporządzenie w sprawie minimalnych wymagań dla systemów teleinformatycznych,
- Rozporządzenie w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej,
- Rozporządzenie w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym,
- Ustawa o narodowym zasobie archiwalnym i archiwach.

Ponieważ część z wyżej wymienionych aktów prawnych dotyczy tylko podmiotów publicznych, analiza aktów prawnych została podzielona na dwie części:

- analiza aktów prawnych odnoszących się do wszystkich podmiotów,
- analiza aktów prawnych dotyczących podmiotów realizujących zadania publiczne.

Wynikiem przeprowadzonej analizy, jest przedstawiony poniżej opis najważniejszych części aktów prawnych odnoszących się do omawianego tematu.

Bezpieczeństwo w rozumieniu aktów prawnych

Przed przystąpieniem do właściwej analizy zadano sobie pytanie, czy tworzone w RP akty prawne rozumieją pojęcie „bezpieczeństwa i ochrony danych” w ten sam sposób. Po przeprowadzeniu analizy opisywanych dokumentów nie można jednoznacznie odpowiedzieć na to pytanie w sposób twierdzący. Wątpliwości wynikają z następujących faktów:

- Analizowane akty prawne powstawały w różnych okresach czasu i opracowywane zostały przez różne zespoły – im więcej zespołów pracujących przy aktach prawnych, tym większe ryzyko, że słowo „bezpieczeństwo” zostanie zinterpretowane w odmienny sposób; oprócz tego nie sposób zauważyć, że im później akt prawny został utworzony bądź nowelizowany, tym dokładniej i precyzyjniej pojęcie „bezpieczeństwo” było w tym akcie wykorzystywane.
- Różne zakresy stosowania aktów prawnych powodują, że wykorzystywane w nich pojęcie „bezpieczeństwa” odnosi się w znacznej większości tylko i wyłącznie do zakresu zdefiniowanego w treści – pojęcie „ochrony danych” rozumiane jest inaczej w Ustawie o ochronie danych osobowych niż w Ustawie o ochronie informacji niejawnej w kontekście przedmiotu ochrony.
- Nie we wszystkich aktach prawnych aspekty bezpieczeństwa zostały potraktowane w należyty sposób – w naszej opinii niektóre akty prawne tylko ogólnie nadmieniają konieczność zachowania ochrony i bezpieczeństwa bez głębszych wyjaśnień i wskazań w tym zakresie.
- Normalizacja znaczenia pojęcia „bezpieczeństwo” pojawiła się dopiero z momentem adaptacji normy ISO 17799:2000 na PN/ISO 17799 – należy zauważyć, że norma PN jest tylko wskazaniem i wytyczną, jej stosowanie nie jest i nie będzie obowiązkowe dopóki nie zostanie to jednoznacznie wskazane w treści ustawy lub rozporządzenia.

Opisane rozbieżności w pojmowaniu i rozumieniu „bezpieczeństwa” w różnych ustawach i rozporządzeniach wymusiły opracowanie i zdefiniowanie przez nas takiego podejścia do analizy, które umożliwiło jej wykonanie w taki sam sposób dla każdego z rozpatrywanych aktów prawnych. Przyjęta przez nas definicja pojęcia „bezpieczeństwa” jest zgodna z polską normą PN/ISO 17799, która opisuje zapewnienie bezpieczeństwa informacji jako zachowanie jej trzech cech:

- poufności,
- integralności,
- dostępności.

Będąc zgodnym z powyższym założeniem podczas analizy aktów prawnych pod kątem opisanych w nich wymagań dla baz danych lub informacji, brano pod uwagę poza zapisami dotyczącymi zabezpieczeń także fragmenty dotyczące udostępniania i wymogów zachowania integralności przy ich przesyłaniu oraz przetwarzaniu.

Akty prawne – dotyczące wszystkich podmiotów

W rozdziale zostały opisane akty prawne dotyczące w sposób ogólny wszystkich podmiotów, o ile podmioty te realizują zadania określone w zakresie tych aktów, lub przetwarzają dane, których dotyczą zapisy w dokumentach. Analizowane akty prawne to:

- Ustawa o ochronie danych osobowych,
- Ustawa o ochronie baz danych,

- Ustawa o świadczeniu usług drogą elektroniczną,
- Ustawa o ochronie informacji niejawnych,
- Ustawa o rachunkowości,
- Prawo Telekomunikacyjne.

W kolejnych podrozdziałach zostaną one omówione dokładniej.

3.1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób, których dane są przetwarzane, niezależnie od sposobu przetwarzania danych (papierowo lub elektronicznie). W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji. Ustawa ta definiuje następujące kwestie:

- Określenie co Ustawa rozumie pod pojęciem dane osobowe (Art. 6).
- Określenie organów ochrony danych osobowych (rozdział 2) w tym wyszczególnienie praw i obowiązków Generalnego Inspektora Ochrony Danych Osobowych (dalej określanego skrótem GIODO) (Art. 12, 14, 18-20) i obowiązków podmiotów względem GIODO (Art. 15).
- Określenie zasad przetwarzania danych osobowych (rozdział 3).
- Wskazanie praw osoby, której dane są przetwarzane (rozdział 4).
- Aspekt zabezpieczania danych osobowych (rozdział 5).
- Obowiązek rejestrowania zbiorów danych osobowych (rozdział 6).
- Zasady przekazywania danych osobowych do państw trzecich (rozdział 7).

Analiza kwestii istotnych

Ustawa prawie w całości (poza artykułami dotyczącymi organizacji i zasad działania GIODO i organów przez niego powołanych) dotyczy analizowanego tematu w kontekście przetwarzania i przechowywania danych osobowych obywateli Rzeczypospolitej Polskiej.

W ramach praw i obowiązków GIODO i organów przez niego powołanych, Ustawa wskazuje prawo GIODO do kontroli podmiotów przetwarzających dane osobowe w zakresie zgodności przetwarzania danych osobowych z zapisami Ustawy. W związku z tym Ustawa w swojej treści nakłada określone obowiązki organizacyjne na te podmioty w celu umożliwienia przeprowadzanie takiej kontroli. Ustawa daje także uprawnienia GIODO do występowania na drodze administracyjnej w razie nieprzestrzegania przez podmioty przetwarzające dane osobowe zapisów Ustawy.

W rozdziale 3 Ustawy opisano zasady organizacyjne przetwarzania danych osobowych, obowiązki wobec podmiotów je przetwarzających, ograniczenia względem informacji jaką można przetwarzać w ramach danych osobowych ze wskazaniem wyjątków, w których możliwe jest przetwarzania tych informacji oraz zasady udostępniania danych osobowych.

Rozdział 4 opisuje jakie czynności organizacyjne muszą być podejmowane przez podmioty przetwarzające dane osobowe w celu umożliwienia realizacji praw osób, których dane są przez te podmioty przetwarzane. Zapisy w artykułach dotyczą głównie określenia zakresu informacji jaką podmiot przetwarzający dane osobowe musi udostępnić osobie, której dane przetwarza.

Bardzo istotnym z punktu widzenia przeprowadzanej analizy jest rozdział 5 Ustawy określający zasady zabezpieczania danych osobowych zarówno w sposób techniczny jak i organizacyjny. Art. 39a określa, że podstawowe warunki organizacyjne jak i techniczne, jakie muszą spełniać

urządzenia i systemy informatyczne służące do przetwarzania danych osobowych są wskazane w rozporządzeniu wydawanym przez ministra właściwego do spraw administracji publicznej.

Rozdział 6 Ustawy opisuje obowiązki organizacyjne podmiotu przetwarzającego dane osobowe w zakresie rejestrowania baz danych do GIODO, w tym wskazanie informacji opisujących bazę danych, jakie należy zgłosić. Rozdział 7 określa zasady przekazywania danych osobowych do państw trzecich – jest to istotne dla rozliczania obywateli Rzeczypospolitej Polskiej pracujących za granicą.

W zakresie zabezpieczeń informacji i baz danych, w których informacje te są przechowywane Ustawa zawiera zasady dotyczące:

- **zbiorów danych osobowych** – w ramach tych zasad określony jest zakres stosowania ustawy (Art. 2, 3, 3a, 6, 40) – dotyczy on głównie aspektów identyfikacji czy w administrowanej bazie danych znajdują się dane osobowe jeżeli tak to jak z nimi postępować.
- **przetwarzania danych osobowych** – w ramach tych zasad określone są:
 - przetwarzanie danych osobowych (rozdz. 3) dotyczące określenia zakresu przetwarzania administrowanych danych, identyfikacji czy jest wymagana i dostępna zgoda osób, których dane dotyczą, weryfikacji kompletności danych i poprawności ich przetwarzania ze zgłoszonym celem i zakresem,
 - udostępnianie danych osobowych (Art. 29, 30, 35) dotyczące mechanizmu udostępniania danych i weryfikacji rejestracji udostępniania danych,
 - przekazywanie danych osobowych (Art. 38) dotyczące określenia formatu przekazywania danych, zakresu i rejestrowania przekazywania danych,
 - powierzenie przetwarzania danych (Art. 31) odnoszące się do przekazywania innym administrowanych danych w celu ich przetwarzania,
- **zabezpieczeń danych osobowych** – w ramach tych zasad określone są:
 - zabezpieczenia organizacyjne (Art. 31, rozdz. 5) dotyczące przeprowadzania analizy ryzyka i identyfikacji zagrożeń, określanie poziomu bezpieczeństwa dla każdego ze zbiorów, nadawanie i zarządzanie upoważnieniami do przetwarzania danych oraz stosowania mechanizmów rozliczalności,
 - dokumentacja (Art. 39a) dotycząca sposobu przetwarzania i zabezpieczania dokumentacji, oraz informacje co powinna taka dokumentacja zawierać i jak nią zarządzać,
 - zabezpieczenia techniczne dotyczące poufności (Art. 39a) opisujące mechanizmy, jakie należy stosować w celu zachowania poufności przetwarzanych zbiorów zawierających dane osobowe; wskazane mechanizmy brzmią następująco:
 - Dostęp do obszarów przetwarzania danych powinien być zabezpieczony i kontrolowany.
 - Należy stosować fizyczne zabezpieczenia instalacji informatycznych, baz danych i nośników zawierających dane osobowe. Równocześnie każdy administrator wykonawczy powinien znać zabezpieczenia stosowane bezpośrednio do swojego systemu.
 - Trzeba wyznaczyć osoby, które będą odpowiedzialne za fizyczne bezpieczeństwo instalacji informatycznych, baz danych i nośników zawierających dane osobowe.
 - Systemy informatyczne powinny posiadać kontrolę dostępu zapewniającą jednoznaczny identyfikację i uwierzytelnianie.
 - Należy określić, w jaki sposób będą weryfikowane nadane uprawnienia dostępu do systemów.

- Do uwierzytelniania użytkowników stosowane powinny być opracowane zasady dotyczące długości i składni haseł oraz określony czas ich ważności.
- Nośniki danych osobowych przed likwidacją, naprawą bądź przekazaniem osobom nieupoważnionym powinny być pozbawione zapisów.
- Do przesyłania danych należy stosować metody kryptograficzne.
- Należy stosować zabezpieczenia fizyczne i logiczne w dostępie do/z sieci publicznej.
- Dla urządzeń przenośnych (laptopów) należy stosować szczególne metody zabezpieczeń.
- zabezpieczenia techniczne dotyczące integralności (Art. 39a) opisujące mechanizmy, jakie należy stosować w celu zachowania integralności przetwarzanych zbiorów zawierających dane osobowe; wskazane mechanizmy brzmią następująco:
 - Należy rejestrować w systemach informacje dotyczące daty wprowadzania do systemu i id użytkownika.
 - Informacje o dostępie i zmianach powinny być rejestrowane automatycznie.
 - W systemach powinny być rejestrowane informacje dotyczące źródła danych, nie od osoby, której one dotyczą.
- zabezpieczenie techniczne dotyczące dostępności (Art. 39a) dotyczące mechanizmów jakie należy stosować w celu zachowania integralności przetwarzanych zbiorów zawierających dane osobowe; wskazane mechanizmy brzmią następująco:
 - Należy stosować systemy bezpieczeństwa (alarmy, system gaszenia) i systemy środowiskowe (temperatura, wilgotność) dotyczące pomieszczeń, w których znajdują się instalacje informatyczne, bazy danych lub nośniki zawierające dane osobowe.
 - Za systemy bezpieczeństwa i systemy środowiskowe musi odpowiadać konkretna osoba.
 - Należy wykonywać kopie zapasowe mające zapewnioną fizyczną ochronę nie gorszą niż dane źródłowe.
 - Dostęp do kopii zapasowych powinien być ograniczony i ściśle kontrolowany.
 - Należy stosować systemy awaryjnego zasilania.
 - Należy opracować plany BCP/DRP, których częścią będzie zabezpieczenie dostępności do danych.
- anonimizacji (Art. 2) dotyczącej zasad niszczenia lub anonimizacji zbiorów, które nie są już przetwarzane.

3.2. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych

Ustawa opisuje zasady ochrony baz danych nie spełniających cech utworów. Ustawa dotyczy baz danych przechowywanych w dowolny sposób. W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa ta definiuje następujące kwestie:

- Określenie definicji bazy danych (Art. 2).
- Określenie jakie bazy danych podlegają ochronie (Art. 5).
- Zasad korzystania z udostępnionej publicznie bazy danych lub jej części (Art. 7 i 8).
- Czasu trwania ochrony bazy danych (Art. 10).

Analiza kwestii istotnych

Ustawa wymienia bazy danych, które podlegają ochronie w tym w szczególności wskazuje na bazy danych utworzone przez podmioty posiadające osobowość prawną.

Jednym z istotnych zapisów w Ustawie jest ten, który mówi, że ochronie opisanej w Ustawie nie podlegają programy komputerowe używane do sporządzenia bazy danych i korzystania z niej.

Ustawa określa także czas obowiązywania ochrony bazy danych na 15 lat od momentu jej utworzenia lub od momentu jej udostępnienia publicznie, o ile to udostępnienie nastąpiło w ciągu 15 lat od jej utworzenia.

3.3. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

Ustawa określa, jakie są obowiązki podmiotu świadczącego usługi drogą elektroniczną, zasady wyłączenia odpowiedzialności usługodawcy oraz zasady ochrony danych osób fizycznych, które korzystają z usługi. W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa ta definiuje następujące kwestie:

- Obowiązek zapewnienia działania systemu informatycznego usługodawcy i działań związanych z zapewnieniem bezpieczeństwa przesyłanych informacji i identyfikacji stron (Art. 7).
- Warunki wyłączenia odpowiedzialności usługodawcy za przechowywane i przetwarzane dane (Art. 13 i 14).
- Obowiązek stosowania Ustawy o ochronie danych osobowych (Art. 16).
- Określenie jakie dane osobowe mogą być przetwarzane (Art. 18).
- Uwarunkowania kiedy usługodawca nie może przetwarzać dane osobowe i jakie dane może przetwarzać po zakończeniu korzystania usługobiorcy z usług świadczonych drogą elektroniczną (Art. 19).
- Warunki kiedy można przetwarzać dane osobowe na potrzeby określenia odpowiedzialności usługobiorcy (Art. 21).

Analiza kwestii istotnych

W zakresie bezpieczeństwa i zapewnienia niezawodności systemu teleinformatycznego Ustawa określa, że usługodawca powinien nieodpłatnie, gdy wymaga tego właściwość usługi, zapewnić korzystanie w usługi świadczonej drogą elektroniczną, tak aby zapewnić ochronę przed nieuprawnionym dostępem do przekazywanej treści wykorzystując w tym celu w szczególności techniki kryptograficzne.

Ustawa poza definiowaniem obowiązków usługodawcy określa także warunki wyłączenia odpowiedzialności usługodawcy w zakresie transmisji danych i ich przechowywania. Dotyczy to głównie sytuacji, w której usługodawca nie jest inicjatorem transmisji danych ani właścicielem przechowywanych danych o charakterze bezprawnym.

Ustawa zwraca uwagę na aspekt przetwarzania danych osobowych usługobiorców w systemie teleinformatycznym usługodawcy. W tym zakresie treść Ustawy stanowi, że:

- należy przestrzegać ustawy o ochronie danych osobowych – o ile opisywana Ustawa nie stanowi inaczej,
- usługodawca może przetwarzać określone w Ustawie dane osobowe, które są niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania umowy między nimi, a także w celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą,

- usługodawca może przetwarzać dane charakteryzujące sposób korzystania z usługi przez usługobiorcę,
- usługodawca nie może przetwarzać danych osobowych po zakończeniu korzystania z usługi świadczonej drogą elektroniczną poza sytuacją dotyczącą: rozliczenia usługobiorcy, reklamy, wyjaśnienia niedozwolonego korzystania z usługi, określenia odpowiedzialności usługobiorcy w przypadku naruszenia przez niego regulaminu.

3.4. Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnej

Ustawa określa zasady ochrony informacji sklasyfikowanej jako tajemnica państwowa lub służbowa. W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa ta definiuje:

- Definicje rodzajów danych, które podlegają ochronie (Art. 2).
- Zasady klasyfikowania informacji niejawnych i nadawania im klauzul tajności (rozdz. 4).
- Zasady zachowania bezpieczeństwa systemów i sieci teleinformatycznych (rozdz. 10).
- Wykaz rodzajów informacji, które mogą stanowić tajemnicę państwową (załącznik nr. 1).

Analiza kwestii istotnych

W pierwszej kolejności Ustawa określa jakie rodzaje danych można sklasyfikować jako informację niejawną. Określone zostały także w niej zasady klasyfikacji informacji w celu jej poprawnej identyfikacji i dalszego przetwarzania.

Ustawa w zakresie zachowania bezpieczeństwa teleinformatycznego dokładnie precyzuje zasady ochrony urządzeń przetwarzających informację, jak i samych informacji. Zasady te można podzielić na następujące obszary:

- **Ochrona fizyczna systemu i sieci** – zasady bezpieczeństwa dotyczące:
 - odpowiedniego umieszczania urządzeń służących do przetwarzania informacji niejawnych w zależności od klauzuli tajności, ilości i zagrożeń dla poufności, integralności i dostępności informacji niejawnych,
 - stosowania środków zapewniających ochronę fizyczną, w szczególności przed:
 - nieuprawnionym dostępem,
 - podglądem,
 - podsłuchem.
- **Role i odpowiedzialności osób** za funkcjonowanie systemów i sieci, przestrzeganie zasad bezpieczeństwa, kontrolę zgodności funkcjonowania sieci i systemów.
- **Ochrona elektromagnetyczna systemu** – zasady bezpieczeństwa dotyczące:
 - umieszczania urządzeń w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej przy uwzględnieniu wyników szacowanego ryzyka,
 - stosowania odpowiednich urządzeń o obniżonym poziomie emisji lub ich ekranowanie i filtrowanie zewnętrznych linii zasilających i sygnałowych.
- **Przekazywanie informacji** na elektronicznych nośnikach z zapewnieniem odpowiedniej ochrony kryptograficznej i zasad opisanych w odrębnych rozporządzeniach.

- **Zapewnienie niezawodności transmisji**, polegającej na zapewnieniu integralności i dostępności informacji niejawnych.
- **Kontrolę dostępu do systemu.**
- **Utworzenie i kontrola dokumentacji** zawierającej m.in. procedury bezpieczeństwa.

3.5. Ustawa o rachunkowości

Ustawa określa zasady rachunkowości oraz tryb badania sprawozdań przez biegłych rewidentów. W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa ta definiuje w rozdziale Ochrona danych (rozdz.8) następujące kwestie:

- wytyczne dotyczące sposobów ochrony danych przetwarzanych przy użyciu komputera (Art. 71),
- zasady przechowywania dowodów księgowych (Art. 73),
- określenie czasu archiwizacji poszczególnych rodzajów danych księgowych (Art. 74).

Analiza kwestii istotnych

Ustawa w odniesieniu do danych rachunkowych przetwarzanych z wykorzystaniem urządzeń komputerowych określa zasady ochrony danych przetwarzanych w tych urządzeniach. W zakresie tych zasad zostały określone następujące elementy:

- sprzęt powinien być chroniony środkami ochrony zewnętrznej,
- należy systematycznie tworzyć kopię zapasową przetwarzanych zbiorów danych na nośnikach zewnętrznych, które powinny być odporne na zagrożenia,
- należy zapewnić trwałość zapisu danych przez czas nie krótszy niż określony w Ustawie,
- należy stosować rozwiązania programowe i organizacyjne w celu ochrony przed nieuprawnionym dostępem do systemów i danych lub ich zniszczeniem.

Ustawa określa w treści informację w jaki sposób mogą być przechowywane dowody księgowe i określa szczegółowo przez jaki czas należy przechowywać poszczególne zbiory danych z podziałem na ich kategorie.

3.6. Ustawa z dnia 16 lipca 2004 r. Prawo Telekomunikacyjne

Ustawa określa zasady wykonywania działalności telekomunikacyjnej przez przedsiębiorców telekomunikacyjnych, w tym warunki przetwarzania danych w telekomunikacji i ochrony tajemnicy telekomunikacyjnej. W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa te definiuje:

- Określenie tajemnicy telekomunikacyjnej i postępowanie z nią (Art. 159).
- Obowiązek stosowania zabezpieczeń wobec zbiorów danych przed ujawnieniem tajemnicy telekomunikacyjnej (Art. 160).
- Określenie danych jakie ma prawo przetwarzać i gromadzić przedsiębiorca telekomunikacyjny (Art. 161).
- Okres w jakim przedsiębiorca telekomunikacyjny może przechowywać dane użytkowników (Art. 164).

- Okres w jakim przedsiębiorca telekomunikacyjny może przechowywać dane teletransmisyjne (Art. 165.) wraz z obowiązkiem stosowania ochrony bezpieczeństwa i poufności tych danych.
- Zasady korzystania z danych o lokalizacji użytkowników (Art. 166).
- Zasady tworzenia „spisu” abonentów i zarządzanie nim (Art. 169).

Analiza kwestii istotnych

Ustawa w swojej treści wyodrębnia cały dział (Dział VII) poświęcony tajemnicy telekomunikacyjnej ochronie danych użytkowników końcowych. Ustawa precyzuje rodzaje przetwarzanych i gromadzonych danych w bazach danych przedsiębiorcy, którego działalność podlega jej regulacjom. Wraz z określeniem rodzajów przetwarzanych danych, zapisy Ustawy wskazują jakie uprawnienia posiada podmiot je przetwarzający w zakresie zarządzania nimi i korzystania z nich.

Ustawa wskazuje na wyjątki w zakresie obowiązywania jej zapisów – wskazanie podmiotów, których dane regulacje nie dotyczą i w jakim zakresie. Wyłączenia z obowiązku przestrzegania prawa dotyczą głównie czynności i podmiotów związanych bezpośrednio z działaniami na rzecz obronności państwa. Aspekty bezpieczeństwa są w Prawie Telekomunikacyjnym poruszane w sposób ogólny, bez wyraźnego wskazania metod i zasad ochrony. Szczególny nacisk Ustawa kładzie na przechowywanie i przetwarzanie danych teletransmisyjnych i ich zabezpieczenie – w zapisach zwrócono uwagę na cechę poufności chronionych danych.

3.7. Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych

Ustawa określa używanie i wykorzystywanie form elektronicznych instrumentów płatniczych do realizacji zobowiązań wynikających z prawa podatkowego. W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa ta definiuje następujące kwestie:

- Obowiązek przestrzegania procedur bezpieczeństwa określonych w umowie pomiędzy agentem rozliczeniowym a akceptantem (Art. 10).
- Zakres danych, jakie powinny być określone w umowie pomiędzy akceptantem (np. Urząd Skarbowy) a agentem rozliczeniowym (np. Bank) (Art. 8).

Analiza kwestii istotnych

Ustawa określa jakie informacje muszą zostać zawarte w umowie pomiędzy akceptantem a agentem rozliczeniowym. w szczególności są to informacje dotyczące stosowania procedury, w tym procedury bezpieczeństwa, oraz obowiązku akceptanta w związku z dokonywaniem operacji.

Ustawa nakłada na akceptanta obowiązek zachowania procedur bezpieczeństwa, które powinny być określone w umowie z agentem rozliczeniowym. W szczególności dotyczy to nieudostępniania danych o posiadaczu lub użytkowniku elektronicznego instrumentu płatniczego osobom niepowołanym oraz do ochrony tegoż elektronicznego instrumentu płatniczego.

Akty prawne dotyczące podmiotów publicznych

W rozdziale zostały opisane akty prawne, które dotyczą podmiotów realizujących zadania publiczne, są to:

- Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne,
- Rozporządzenie w sprawie minimalnych wymagań dla systemów teleinformatycznych,

- Rozporządzenie w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej,
- Rozporządzenie w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym,
- Ustawa o narodowym zasobie archiwalnym i archiwach.

W kolejnych podrozdziałach zostały one opisane dokładniej.

4.1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

Ustawa określa zasady:

- ustalania minimalnych wymagań dla systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych oraz dla rejestrów publicznych i wymiany informacji w formie elektronicznej,
- dostosowywania obecnie używanych systemów teleinformatycznych do wymagań dla systemów teleinformatycznych,
- dostosowywania rejestrów publicznych i wymiany informacji do określonych wymagań,
- kontroli projektów informatycznych o publicznym zastosowaniu,
- wymiany informacji drogą elektroniczną,
- ustalania i publikacji specyfikacji stosowanych rozwiązań.

W zakresie zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa ta definiuje następujące kwestie:

- Obowiązek spełniania przez systemy teleinformatyczne minimalnych wymagań dla systemów teleinformatycznych, rejestrów publicznych i transmisji danych (Art. 13 i 14).
- Obowiązek udostępniania danych z prowadzonego rejestru podmiotom publicznym lub realizującym zadania publiczne (Art. 15).
- Obowiązek zgłaszania do krajowej ewidencji danych dotyczących prowadzonego rejestru publicznego i danych dotyczących wykorzystywanego systemu teleinformatycznego (Art. 20).

Analiza kwestii istotnych

W Ustawie zawarto zapisy, w których mowa, że systemy teleinformatyczne wykorzystywane do realizacji zadań publicznych muszą spełniać minimalne wymagania dla systemów teleinformatycznych w niej wskazane. Dodatkowo na podmiot wykorzystujący system teleinformatyczny nakłada się obowiązek:

- spełniania przez systemy wykorzystywane do wymiany danych zasady równego traktowania rozwiązań informatycznych,
- publikowania w BIP lub inny sposób informacji dotyczących wykorzystywanych formatów dokumentów, formatów danych, protokołów komunikacyjnych oraz szyfrujących.

W zakresie podmiotów publicznych prowadzących rejestr publiczny Ustawa zobowiązuje je do spełniania minimalnych wymagań dla systemów teleinformatycznych, jeżeli rejestr ten jest prowadzony w tych systemach oraz spełniania minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

Ustawa określa obowiązek i zasady udostępniania danych z rejestru publicznego wskazując na rozporządzenie Prezesa Rady Ministrów, które ma zawierać szczegóły w tym zakresie.

Zgodnie z Ustawą podmioty publiczne wykorzystujące systemy teleinformatyczne i prowadzące rejestry publiczne powinny zgłosić je do krajowej ewidencji wraz ze wskazanymi w Ustawie informacjami opisującymi te systemy.

4.2. Rozporządzenie w sprawie minimalnych wymagań dla systemów teleinformatycznych

Rozporządzenie określa minimalne wymagania dla systemów teleinformatycznych, w szczególności systemy te powinny (§2):

- spełniać właściwości i cechy w zakresie funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, określone w normach ISO zatwierdzonych przez krajową jednostkę normalizacyjną, na etapie projektowania, wdrażania i modyfikowania tych systemów,
- być wyposażone w składniki sprzętowe i oprogramowanie:
 - umożliwiające wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych za pomocą protokołów komunikacyjnych i szyfrujących określonych w załączniku nr 1 do rozporządzenia, stosownie do zakresu działania tych systemów,
 - zapewniające dostęp do zasobów informacji udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych przy wykorzystaniu formatów danych określonych w załączniku nr 2 do rozporządzenia.

Rozporządzenie nakłada na podmiot publiczny wykorzystujący system teleinformatyczny obowiązek opracowania i wdrożenia polityki bezpieczeństwa (§3 pkt. 1) dla tego systemu z uwzględnieniem Polskich Norm z zakresu bezpieczeństwa informacji (§3 pkt. 2).

4.3. Rozporządzenie w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej

Rozporządzenie określa minimalne wymagania, jakie powinny spełniać rejestry publiczne w zakresie zapewnienia spójności działań z innymi systemami teleinformatycznymi, jak również wymiany informacji pomiędzy rejestrami publicznymi. Rozporządzenie w załączniku określa definicje cech informacyjnych i obowiązek korzystania z nich przez podmioty prowadzące rejestr publiczny i wymianę informacji w formie elektronicznej.

4.4. Rozporządzenie w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym

Rozporządzenie określa sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrze publicznym, podmiotom realizującym zadania publiczne.

W zakresie bezpieczeństwa danych dokument nakłada obowiązki na podmiot prowadzący rejestr o informowaniu w sposób powszechnie dostępny, w tym w Biuletynie Informacji Publicznej, o warunkach zabezpieczeń technicznych i organizacyjnych niezbędnych do uzyskania dostępu do danych zgromadzonych w rejestrze. Także podmiot, któremu udostępniono dane zgromadzone w rejestrze, ma obowiązek zabezpieczenia otrzymanych danych przed dostępem osób nieupoważnionych lub nieuprawnioną zmianą ich zawartości oraz przed ich wykorzystaniem niezgodnym z celem, dla którego zostały uzyskane.

Według rozporządzenia podmiot, któremu udostępniono dane zgromadzone w rejestrze, odpowiada za bezpieczeństwo i integralność uzyskanych danych.

4.5. Ustawa z dnia 14 lipca 1983 r. – o narodowym zasobie archiwalnym i archiwach

Ustawa definiuje pojęcie materiału archiwalnego, przedstawia informacje na temat narodowego zasobu archiwalnego, jego podziału i działalności archiwalnej w jego zakresie. Reguluje ponadto sprawy dotyczące niepaństwowego zasobu archiwalnego oraz postępowanie materiałami archiwalnymi. Ustawa ta wymienia również przepisy karne dotyczące postępowania z materiałami archiwalnymi.

Z punktu widzenia zabezpieczeń baz danych i przechowywanych w nich informacji Ustawa reguluje kwestię gromadzenia i przechowywania wszelkiej dokumentacji obsługiwanej przy użyciu systemu, z uwzględnieniem elektronicznej formy dokumentów. W szczególności ustawa pozwala zaklasyfikować dane gromadzone w systemie do narodowego zasobu archiwalnego (art. 1 i 15 ust. 1), uwzględnia potrzebę nałożenia szczególnych wymagań wynikających z elektronicznej postaci dokumentów i archiwum (art. 5 ust.2). Określa zasady tworzenia archiwów zakładowych dla dokumentów nie podlegających narodowemu zasobowi archiwalnemu (art. 33) wyznaczając zakres odpowiedzialności za zgromadzone zasoby (art. 34) oraz reguluje działanie archiwum zakładowego (art. 35).

Podsumowanie

Obecnie obowiązuje duża liczba aktów prawnych, których zapisy dotyczą baz danych i informacji w nich przechowywanych w szczególności w kontekście bezpieczeństwa. Akty te różnią przede wszystkim zakresy stosowania w aspekcie danych, których dotyczą jak i podmiotów, które przetwarzają te dane. W większości analizowanych aktów prawnych obowiązek stosowania zabezpieczeń i ochrony danych jest potraktowany bardzo ogólnie, wręcz na poziomie jednego zdania lub akapitu w stylu: „należy zadbać o stosowanie zabezpieczeń przetwarzanych danych”. Tylko niektóre z analizowanych dokumentów wskazują na konkretne mechanizmy i sposoby zabezpieczeń. Pytanie, na które muszą odpowiadać sobie administratorzy brzmi następująco: w jaki sposób spełnić zapisy aktu prawnego, gdy nie ma w nim wskazanych informacji, jaki stan jest uznawany za zgodny z danym aktem? Proponowanym rozwiązaniem tegoż problemu jest wykonanie następujących czynności przez administratorów:

- Identyfikacja rodzaju danych przechowywanych w ich bazach danych.
- Określenie charakterystyki prowadzonej działalności przez podmiot, który jest właścicielem bazy danych, w tym zakresu świadczonych usług, podmiotów współpracujących.
- Określenie na podstawie powyższej analizy które z omówionych w artykule aktów prawnych dotyczą administrowanej przez niego bazy i informacji.
- Weryfikacja, czy bazy danych spełniają opisane wymagania z zakresu bezpieczeństwa i wdrożenie wymaganych mechanizmów, a w przypadku ogólnych zapisów o stosowaniu ochrony i zabezpieczeń, skorzystanie z normy PN/ISO 17799 w zakresie wyboru metod ochrony i ich wdrożenie.

Podjęcie powyższych kroków powinno w efekcie zapewnić zgodność administrowanych baz danych z obowiązującym w Polsce prawem w tym zakresie.

Bibliografia

- [1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- [2] Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych
- [3] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną
- [4] Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych
- [5] Ustawa z dnia 16 lipca 2004 r. Prawo Telekomunikacyjne
- [6] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnej
- [7] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne
- [8] Rozporządzenie w sprawie minimalnych wymagań dla systemów teleinformatycznych
- [9] Rozporządzenie w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym
- [10] Rozporządzenie w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym
- [11] Ustawa z dnia 14 lipca 1983 r. - o narodowym zasobie archiwalnym i archiwach

