

# Magdalena Rzemieniak

---

## Wybrane aspekty prawne baz danych oraz danych osobowych w kontekście rozwoju społeczeństwa informacyjnego

---

Ekonomiczne Problemy Usług nr 88, 782-790

---

2012

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MAGDALENA RZEMIENIAK

Politechnika Lubelska

## WYBRANE ASPEKTY PRAWNE BAZ DANYCH ORAZ DANYCH OSOBOWYCH W KONTEKŚCIE ROZWOJU SPOŁECZEŃSTWA INFORMACYJNEGO

### Wprowadzenie

Dla społeczeństwa informacyjnego, w którym szczególnym dobrem niematerialnym stała się informacja, regulacje prawne w zakresie baz danych i danych osobowych mogą stanowić bariery rozwojowe. Celem artykułu jest prezentacja regulacji prawnych w zakresie baz danych i danych osobowych oraz próba uświadomienia, że regulacje te muszą jednocześnie ewoluować, by stawać się zabezpieczeniem dla zagrożeń dla bezpieczeństwa danych osobowych przetwarzanych w systemach teleinformatycznych.

Skuteczność działań informacyjnych zależy m.in. od doboru właściwej bazy danych. Kotler definiuje to pojęcie w następujący sposób: „baza danych o klientach [to] uporządkowany zbiór wyczerpujących danych o istniejących i potencjalnych klientach obejmujących dane geograficzne, demograficzne, psychograficzne i dotyczące zachowań nabywczych<sup>1</sup>.”

### 1. Problematyka baz danych w rozprzestrzeleniu informacji z prawnego punktu widzenia

Bazy danych są podstawowym elementem umożliwiającym prowadzenie skutecznych działań informacyjno-promocyjnych. Regulacje z nimi związane znajdują się w dwóch aktach prawnych. Pierwszym jest ustawa z dnia 4 lutego 1994 r.

---

<sup>1</sup> P. Kotler, *Marketing. Podręcznik europejski*, PWE, Warszawa 2002, s. 1042.

o prawie autorskim i prawach pokrewnych z późniejszymi zmianami. Wspomniany akt prawny chroni jednak wyłącznie zbiory informacji zawierające pewien element oryginalności. Dodatkowym warunkiem ograniczającym zastosowanie powyższej ustawy jest wymóg wykorzystania twórczego doboru, układu lub zestawienia elementów<sup>2</sup>. Opisane cechy rzadko występują w odniesieniu do baz marketingowych. Zbiory tworzone na potrzeby marketingowo-promocyjne składają się z wielu różnych informacji demograficznych, geograficznych, psychograficznych i innych, a ich ułożenie trudno uznać za oryginalne. Każda firma stara się pogrupować dane w sposób, który jak najbardziej ułatwia dysponowanie nimi. Ostatecznie większość baz danych wygląda i funkcjonuje podobnie. Drugim ważnym aktem prawnym jest ustawa z dnia 27 lipca 2001 r. o ochronie baz danych z późniejszymi zmianami. Dotyczy ona niemal wszystkich baz danych wykorzystywanych w działaniach marketingu bezpośredniego. Głównym celem wspomnianej ustawy jest przede wszystkim ochrona nakładów, jakie przedsiębiorca poniósł na zebranie informacji i stworzenie z nich odpowiedniego zbioru. Warto zwrócić uwagę na fakt, że omawiany akt prawny chroni bazę danych jako całość. Regulacje dotyczące ochrony poszczególnych elementów danego zbioru zawierają odrębne ustawy<sup>3</sup>.

## 2. Baza danych w rozumieniu ustawy o ochronie baz danych oraz elementy bazy danych objęte ochroną prawną

Ustawa o ochronie baz danych ma ogromne znaczenie dla wszystkich osób, które z takich zasobów korzystają. Omawiane pojęcie jest w niej definiowane w następujący sposób: „(...) baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości (...)”<sup>4</sup>. Zatem aby baza danych mogła zostać objęta ochroną prawną, powinna spełniać pewne warunki<sup>5</sup>.

---

<sup>2</sup> Por. art. 3 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (DzU 1994 nr 24, poz. 83 ze zm.).

<sup>3</sup> Por. X. Konarski, M. Woźniacka, *Prawo marketingu bezpośredniego*, Stowarzyszenie Marketingu Bezpośredniego, <http://www.nf.pl/Artykul/9676/>, (data dostępu: 13.01.2012).

<sup>4</sup> Art. 2 ust. 1 ustawy z dnia z dnia 27 lipca 2001 r. o ochronie baz danych ze zm. (DzU 2001 nr 128, poz. 1402 ze zm.).

<sup>5</sup> Po pierwsze musi stanowić określony zbiór informacji lub materiałów, a wszystkie jej elementy powinny być uporządkowane według ustalonej metody. Kolejnym wymogiem jest konieczność poniesienia przez producenta istotnego nakładu inwestycyjnego związanego z jej sporządzeniem, weryfikacją albo prezentacją. Bazy danych wykorzystywane do działań informacyjno-promocyjnych najczęściej spełniają wszystkie opisane wyżej kryteria. Przed szerszym omówieniem zagadnień znajdujących się w ustawie warto wyjaśnić pojęcie producenta. Jest to

Zgodnie z treścią ustawy ochronie podlega cała utworzona baza danych lub jej istotna część, ze względu na jakość bądź ilość zawartych w niej elementów<sup>6</sup>. W tym przypadku „istotność” części bazy danych będzie zależała zarówno od jej wielkości, jak i jakości, gdyż nawet niewielka ilość informacji może posiadać wysoką wartość ekonomiczną. Ustawa gwarantuje producentowi bazy danych wyłączność na korzystanie z niej lub jej istotnej części. Jeżeli inne podmioty wyrażą chęć korzystania ze zbiorów informacji chronionych ustawą, będą zmuszone do uiszczenia odpowiedniej opłaty w celu zakupu licencji lub odpowiedniego pozwolenia. Czynności takie jak kopiowanie danych, zapisywanie ich na przenośnych nośnikach informacji czy drukowanie mogą być wykonywane jedynie przez wspomnianego producenta lub za jego zgodą. Wyłączność obejmuje również wtórne wykorzystywanie danych polegające na publicznym udostępnianiu<sup>7</sup>.

Czas ochrony bazy danych wynosi 15 lat. Jeżeli w tym czasie zbiór zostanie udostępniony publicznie, wspomniany okres wygaśnie dopiero po 15 latach od momentu pierwszego udostępnienia. W przypadku istotnej modyfikacji ilości, treści lub jakości danych zawartych w zbiorze czas obowiązywania ochrony jest liczony odrębnie<sup>8</sup>.

### 3. Konsekwencje nieprzestrzegania regulacji prawnych dotyczących baz danych

Ustawa o ochronie baz danych nie tylko reguluje działania w zakresie własności i możliwości korzystania z baz danych, ale również określa kary, jakie zostaną nałożone na osoby lub instytucje niestosujące się do zamieszczonych w niej postanowień. Zgodnie z art. 11 w razie naruszenia bazy danych producent może żądać:

- zaprzestania prowadzenia działań niezgodnych z prawem,
- usunięcia skutków spowodowanych wspomnianymi czynnościami,
- naprawy wyrządzonej szkody,
- wydania korzyści, jakie udało się uzyskać podczas korzystania ze zbioru.

Dodatkowo pokrzywdzony może domagać się wydania odpowiedniego oświadczenia w prasie lub podania do publicznej wiadomości orzeczenia sądu wy-

---

osoba fizyczna lub firma, która finansowała powstanie bazy danych lub poniosła inne nakłady inwestycyjne związane z jej utworzeniem. Por. art. 2, *ibidem*.

<sup>6</sup> Por. art. 6, *ibidem*.

<sup>7</sup> Przykładem nieistotnej części bazy danych jest np. rozkład jazdy autobusów komunikacji miejskiej. Pomimo że dane zostały uznane za nieistotne, ustawa przewiduje co do nich pewne regulacje. Będzie to przede wszystkim zakaz systematycznego pobierania i wtórnego wykorzystywania (publiczne udostępnianie informacji) niezgodnie z przeznaczeniem. Wspomniany zapis został ustanowiony, aby zapobiec naruszeniu interesów producenta, dlatego operacja polegająca na odtworzeniu cudzej bazy danych poprzez systematyczne kopiowanie jej nieistotnych (w rozumieniu ustawy) elementów będzie działaniem sprzecznym z prawem. Por. X. Konarski, M. Woźnicka, *Prawo...*, *op. cit.*, <http://www.nf.pl/Artykul/9716/> (data dostępu: 13.01.2012).

<sup>8</sup> Zob. art. 10 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych, *op. cit.*

danego w związku z omawianą sprawą. Sąd może również zobowiązać jednostkę działającą sprzecznie z ustawą do zapłaty określonej sumy pieniężnej na rzecz producenta<sup>9</sup>.

Kolejną sankcją nakładaną przez ustawę na nieuczciwe jednostki jest kara grzywny. Poniesie ją każdy, kto bez uprawnień będzie pobierał dane w całości lub w istotnej części i spróbuje je wykorzystać w celu zdobycia korzyści majątkowych<sup>10</sup>.

#### 4. Pojęcie danych osobowych

Według ustawy dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, czyli takiej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacjami umożliwiającymi określenie tożsamości nie są natomiast dane, których wykorzystanie w celu identyfikacji wymagałoby poświęcenia nadmiernych kosztów, czasu lub działań<sup>11</sup>.

Z przytoczonej definicji wynika, że za dane osobowe nie będą uważane ogólne pojedyncze informacje, takie jak na przykład nazwa ulicy z podanym numerem bloku. Jeżeli wspomniany zestaw danych zostanie wzbogacony o konkretny numer mieszkania oraz imię i nazwisko określonej osoby, to zacznie podlegać ochronie omawianej ustawy. Wyjątek stanowi natomiast numer PESEL, który dzięki swojej konstrukcji umożliwi dosyć dokładną identyfikację właściciela<sup>12</sup>. Z tego powodu jest chroniony przez prawo nawet wtedy, gdy występuje samodzielnie<sup>13</sup>. Warto także wspomnieć o danych szczególnie chronionych, czyli takich, które mogą być przetwarzane wyłącznie po spełnieniu szeregu warunków nakładanych przez wspomniany akt prawny. Będą to takie informacje jak:

---

<sup>9</sup> Zob. art.11, *ibidem*.

<sup>10</sup> Zob. art. 12, *ibidem*.

<sup>11</sup> Art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 1997 nr 133, poz. 883 ze zm.).

<sup>12</sup> Nr PESEL składa się z 11 cyfr, z których sześć pierwszych oznacza zakodowaną w określony sposób datę urodzenia, a przedostatnia określa płeć właściciela (cyfry parzyste oznaczają płeć żeńską, a nieparzyste męską).

<sup>13</sup> Zazwyczaj adresy e-mail nie są traktowane jako dane osobowe. Wyjątek stanowią sytuacje, gdy w ich treści zostanie umieszczone imię i nazwisko właściciela (np. magdalena.rzemieniak@pollub.pl). Warto podkreślić, że przepisy zawarte w ustawie o ochronie danych osobowych stosuje się jedynie w odniesieniu do danych dotyczących osób fizycznych. Przewidziana w niej ochrona nie będzie dotyczyła firm ani osób zmarłych. Por. *ABC ochrony danych osobowych*, red. A. Kowalik, Wydawnictwo Sejmowe, Warszawa 2007, s. 10–11, <http://www.giodo.gov.pl/485/> (data dostępu: 14.01.2012).

- przynależność wyznaniowa, partyjna lub związkowa,
- stan zdrowia,
- kod genetyczny,
- nałogi,
- życie seksualne,
- informacje o skazaniach, orzeczeniach ukarania, mandatach karnych i innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym<sup>14</sup>.

## 5. Przetwarzanie zbioru danych osobowych w społeczeństwie informacyjnym

Nie każde zestawienie danych będzie można określić mianem zbioru danych osobowych. Według ustawy jest to zestaw informacji o charakterze osobowym posiadający strukturę. Nie ma znaczenia, czy będzie on rozproszony, czy też zostanie podzielony funkcjonalnie, powinien jednak umożliwiać wyszukiwanie informacji według różnych kryteriów<sup>15</sup>. Zbiorami danych będą zatem wszelkiego rodzaju materiały w formie akt, np. sądowe lub policyjne, informacje, które pracodawca gromadzi o zatrudnionych osobach, oraz wszelkie inne zestawienia odpowiadające definicji wynikającej z ustawy. Sposób przechowywania (elektroniczny lub na papierze) nie będzie miał w tym wypadku znaczenia.

Proces przetwarzania danych osobowych tak samo jak pozostałe operacje z nimi związane jest ściśle regulowany przez omawianą ustawę. Podstawowe zasady działania określono w art. 26 ust. 1 jako obowiązki administratora danych. Należy do nich przede wszystkim dołożenie szczególnej staranności w celu zapewnienia ochrony osobom, których dotyczą zebrane informacje. W związku z powyższym administrator musi się stosować do kilku głównych zasad. Pierwszą z nich jest *zasada legalności*, która nakazuje przetwarzanie danych zgodnie z prawem. Oznacza to konieczność spełnienia przynajmniej jednej z przesłanek legalności wymienionych w art. 23 ustawy o ochronie danych osobowych<sup>16</sup>. „Przetwarzanie danych jest dopuszczalne w konkretnych przypadkach”<sup>17</sup>.

---

<sup>14</sup> Zob. art. 27 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, *op. cit.*

<sup>15</sup> Zob. art. 7 pkt 1, *ibidem*.

<sup>16</sup> Por. *ABC wybranych zagadnień ustawy o ochronie danych osobowych*, red. A. Rudnicki, Wyd. Sejmowe, Warszawa 2007, s. 12–13, <http://www.giodo.gov.pl/485/> (data dostępu: 10.01.2012).

<sup>17</sup> Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego

Szczególną uwagę warto zwrócić na punkt 5. Za prawnie usprawiedliwiony cel ustawa uznaje między innymi działania prowadzone w ramach działalności informacyjno-promocyjnej związanej z promocją produktów lub usług oferowanych przez administratora<sup>18</sup>. Warto zauważyć, że punkt ten dotyczy jedynie działań związanych z prowadzeniem tzw. „marketingu własnego”. W przypadku działań informacyjno-promocyjnych prowadzonych na rzecz innych firm – tzw. „marketingu cudzego” – konieczne będzie pozyskanie specjalnej zgody na przetwarzanie danych osobowych<sup>19</sup>. Omawiana zasada legalności zabrania zbierania danych osobowych w sposób sprzeczny z prawem. Zakazuje stosowania działań ukrytych, prowadzonych przy użyciu podsłuchu lub wariografu oraz takich, które w jakikolwiek sposób ingerowałyby w tajemnicę korespondencji. Zgoda na przetwarzanie danych osobowych musi być wyrażona na piśmie, nie może być w żaden sposób „domniemana lub dorozumiana z oświadczenia woli o innej treści”<sup>20</sup>. Dokument należy tak sporządzić, aby nie budził wątpliwości co do celu wykorzystania danych, a osoba podpisująca go miała pełną świadomość, na co się zgadza. Przykładową klauzulę zgody na przetwarzanie danych osobowych przedstawiono na rysunku 1.

Kolejną zasadą wyznaczającą kierunek działań administratora jest *zasada celowości*. Według niej dane osobowe mogą być zbierane tylko pod warunkiem zdefiniowania celu ich gromadzenia. W myśl tej reguły zgromadzone informacje nie mogą być wykorzystywane do realizacji innych niż wymienione w zgodzie działań. Następną zasadą dotyczącą *merytorycznej poprawności* danych nakazuje administratorowi każdorazową ocenę wiarygodności źródła, z którego pochodzą informacje, nadzorowanie zgodności danych ze stanem faktycznym oraz informowanie o wprowadzonych zmianach wszystkich, którzy korzystają z zarządzanej przez niego bazy danych. W praktyce oznacza to zakaz dysponowania informacjami, które są nieprawdziwe, nieaktualne lub niekompletne. Kolejną regulacją jest *zasada adekwatności*, nakazująca zbieranie tylko tych danych, które są niezbędne do realizacji celu określonego przez administratora. Informacje nie mogą być gromadzone ze względu na możliwość ewentualnego wykorzystania w przyszłości, czyli „na zapas”. Ostatnią zasadą, o której warto wspomnieć jest *ograniczenie w czasie*. Zgodnie z tą regulacją dane mogą być przechowywane przez administratora tylko do momentu osiągnięcia wyznaczonego celu<sup>21</sup>.

---

oraz gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Art. 23 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, *op. cit.*

<sup>18</sup> Art. 23, ust. 4, pkt 1, *ibidem*.

<sup>19</sup> Por. X. Konarski, M. Woźniacka, *Prawo...*, *op. cit.*, <http://www.nf.pl/Artykul/9855/> (data dostępu: 13.01.2012).

<sup>20</sup> II SA 2135/02 – Wyrok NSA, <http://orzeczenia.nsa.gov.pl/doc/6B17392974> (data dostępu: 11.01.2012).

<sup>21</sup> Por. *ibidem*, s. 16–18.

Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie obejmującym imię, nazwisko i adres zamieszkania, przez XYZ Sp. z o.o. z siedzibą w Warszawie (00-111), ul. Kwiatowa 1, w celach przesyłania ofert marketingowych, jak również na przekazywanie ich innym podmiotom.

Warszawa, dnia 5 stycznia 2012 r.

Anna Iksińska

Rys. 1. Przykładowa klauzula zgody na przetwarzanie danych osobowych

Źródło: *ABC wybranych zagadnień ustawy o ochronie danych osobowych*, red. A. Rudnicki, Wyd. Sejmowe, Warszawa 2007, s. 16, <http://www.giodo.gov.pl/485/> (data dostępu: 10.01.2012).

## 6. Zabezpieczenie danych osobowych

W związku z wysoką wartością informacji, jakimi są dane osobowe, ustawa nakłada na administratora obowiązki związane z ich zabezpieczeniem. Zgodnie z art. 36 ust. 1 jest on zobowiązany do zastosowania środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanym informacjom, „w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem”<sup>22</sup>.

W dzisiejszych czasach przeważająca część baz danych osobowych jest przechowywana w systemach informatycznych<sup>23</sup>.

Obowiązki nałożone na administratora danych można podzielić na organizacyjne i techniczne. Pierwsza grupa jest związana z kontrolowaniem oraz nadzorowaniem dostępu do danych. Można do niej zaliczyć np. konieczność nadawania uprawnień przez administratora osobom, które mają być dopuszczone do zbioru danych albo obowiązek związany z ewidencjonowaniem takich użytkowników. Druga grupa obowiązków wiąże się głównie z danymi przechowywanymi w systemach informatycznych i jest szczegółowo opisana we wspomnianym rozporządzeniu z dnia 29 kwietnia 2004 r.<sup>24</sup> We wspomnianym akcie prawnym znajdują się

<sup>22</sup> Art. 36 ust. 1 ustawy z dnia 29 sierpnia 1994 r. o ochronie danych osobowych, *op. cit.*

<sup>23</sup> Dokumentem, który reguluje sytuację prawną związaną z przetwarzaniem danych we wspomnianych systemach, jest 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 (DzU nr 100, poz. 1024). W tym miejscu warto zdefiniować pojęcie bezpieczeństwa informacji, które w przypadku systemów teleinformatycznych będzie tożsame z ochroną danych. Przez to sformułowanie „(...) należy rozumieć zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności”. *Ibidem*, s. 6.

<sup>24</sup> Por. X. Konarski, M. Woźniacka, *Prawo...*, *op. cit.*, <http://www.nf.pl/Artykul/9955/> (data dostępu: 13.01.2012).



m.in. informacje o sposobie prawidłowego konstruowania struktur baz danych oraz wytyczne związane ze stosowanymi aplikacjami. Pojawiają się również zagadnienia takie jak trójpoziomowy podział bezpieczeństwa systemów informatycznych oraz wytyczne związane z polityką bezpieczeństwa. Ważnym wymogiem, jaki omawiane rozporządzenie nakłada na administratora, jest konieczność sporządzenia instrukcji określającej sposób zarządzania systemem informatycznym<sup>25</sup>. Konieczna jest zatem rejestracja zbioru danych osobowych<sup>26</sup>.

## Podsumowanie

Regulacje prawne w zakresie informacyjno-promocyjnym mogą dla społeczeństwa informacyjnego stanowić zarówno bariery rozwojowe, jak i być źródłem wielu zabezpieczeń. Dynamiczny rozwój technologii umożliwił niestety działania nieetyczne, tj. ataki crackerów, podsłuch, manipulacje, podstawienie czy phishing. Znajomość regulacji prawnych w danym obszarze pozwala na ochronę danych osobowych oraz na świadome działania informacyjno-promocyjne.

## Literatura

1. *ABC ochrony danych osobowych*, red. A. Kowalik, Wydawnictwo Sejmowe, Warszawa 2007, s. 10–11, <http://www.giodo.gov.pl/485/> (data dostępu: 14.01.2012).
2. *ABC wybranych zagadnień ustawy o ochronie danych osobowych*, red. A. Rudnicki, Wydawnictwo Sejmowe, Warszawa 2007, s. 12–13, <http://www.giodo.gov.pl/485/> (data dostępu: 10.01.2012).
3. Kotler P., *Marketing. Podręcznik europejski*, PWE, Warszawa 2002.
4. Konarski X., Woźniacka M., *Prawo marketingu bezpośredniego*, Stowarzyszenie Marketingu Bezpośredniego, <http://www.nf.pl/Artykul/9676/> (data dostępu: 13.01.2012).

---

<sup>25</sup> Szerzej na ten temat w: *ABC bezpieczeństwa...*, *op. cit.*

<sup>26</sup> Zgodnie z art. 40 ustawy o ochronie danych osobowych obowiązkiem administratora jest zgłoszenie zbioru danych do Generalnego Inspektora Ochrony Danych osobowych w celu rejestracji. Przypadki, w których opisany wyżej sposób postępowania nie obowiązuje, zostały wyszczególnione w art. 43 ust. 1 wspomnianego aktu prawnego. Zgłoszenie odbywa się poprzez wypełnienie odpowiedniego formularza zamieszczonego w rozporządzeniu do ustawy. Taki dokument może zostać dostarczony osobiście, wysłany pocztą lub uzupełniony i przekazany drogą elektroniczną, o ile dany podmiot posiada podpis elektroniczny. Każda zmiana dotycząca zbioru danych również będzie wymagała zgłoszenia. Administrator może rozpocząć przetwarzanie danych od momentu zgłoszenia zbioru, chyba że są to informacje szczególnie chronione. Wtedy podmiot zgłaszający jest zobowiązany wstrzymać się do momentu ukończenia procesu rejestracji i uzyskania odpowiedniego zaświadczenia.

5. [www.e-podatnik.pl/arttykul/doradca\\_podatnika/3597/Umowy\\_nienazwane\\_w\\_obrocie\\_gospodarczym.html](http://www.e-podatnik.pl/arttykul/doradca_podatnika/3597/Umowy_nienazwane_w_obrocie_gospodarczym.html) (data dostępu: 10.01.2012).
6. [www.giodo.gov.pl/138/id\\_art/1975/j/pl/](http://www.giodo.gov.pl/138/id_art/1975/j/pl/) (data dostępu: 10.01.2012).
7. II SA 2135/02 – Wyrok NSA, <http://orzeczenia.nsa.gov.pl/doc/6B17392974> (data dostępu: 11.01.2012).
8. Art. 2 ust. 1 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych ze zm. (DzU 2001 nr 128, poz. 1402 ze zm.).
9. Art. 3 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (DzU 1994 nr 24, poz. 83 ze zm.).
10. Art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 1997 nr 133, poz. 883 ze zm.).
11. Art. 10 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych.
12. Art. 7 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
13. Art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
14. Art. 27 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
15. Art. 32 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
16. Art. 32 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
17. Art. 33 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

## **SELECTION LEGAL ASPECTS OF DATABASES AND DATA DEVELOPMENT IN THE CONTEXT OF THE INFORMATION SOCIETY**

### **Summary**

For the information society, in which a particular intangible asset has become the information, legal regulations in the field of databases and personal information may constitute a barrier to development. At the same time these regulations must evolve to become security for threats to the security of personal data processed in ICT systems.

*Translated by Magdalena Rzemieniak*