

# Ustawa o ochronie danych osobowych a bazy danych Oracle

*Wojciech Dworakowski (SecuRing) – wojtekd@securing.pl*

*Uwaga: Poniższego artykułu i towarzyszącej mu prezentacji nie należy traktować jako wyczerpującej listy kontrolnej dotyczącej zgodności bazy danych z ustawą o ochronie danych osobowych. Artykuł i prezentacja są siłą rzeczy mocno wybiórcze. Celem autora jest raczej zwrócenie uwagi twórców i administratorów baz danych i aplikacji na problem zgodności z ustawą o ochronie danych osobowych.*

Ustawa o ochronie danych osobowych obowiązuje w naszym kraju już od kilku lat. 01 maja 2004, wraz z naszym wejściem do Unii Europejskiej weszła w życie nowelizacja tej ustawy. Instytucje przetwarzające dane osobowe w dniu wejścia nowych regulacji miały okres karencji do 1 listopada 2004 aby przystosować się do nowych wymagań. Znowelizowana ustawa narzuca na administratorów danych dość konkretne wymagania techniczne dla systemów informatycznych w tym dla baz danych i interfejsów aplikacyjnych. Niespełnienie wymagań ustawowych może narazić firmę na poważne konsekwencje, włącznie z nakazem usunięcia zbioru danych które są przetwarzane nieprawidłowo (ustawa przewiduje nawet karę pozbawienia wolności).

Tekst ustawy narzuca wymagania jakie musi spełniać sposób przetwarzania danych osobowych. Wśród tych wymagań pokazną część zajmują wymagania dotyczące systemów informatycznych. Podzbiorem tych wymagań są znowu wymagania dotyczące baz danych i aplikacji. Na tych właśnie wymaganiach skupimy się.

## Dane osobowe

Na początek – krótkie wprowadzenie do problemu. Przede wszystkim musimy sobie zadać pytanie czy nasza baza danych / aplikacja podlega ustawie o ochronie danych osobowych?

Po pierwsze – co to są dane osobowe? Art. 6 ustawy mówi że:

1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Osobą możliwą do zidentyfikowania jest osoba, 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.
3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Po drugie – kto musi się stosować do wymogów ustawy? Upraszczając – wszyscy z wyjątkiem m.in.(Art 3a Ustawy):

- osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych,

- działalności dziennikarskiej, literackiej lub artystycznej (chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą)

Po trzecie – obowiązek rejestracji w GIODO.

Zbiór danych należy zgłosić do Generalnego Inspektora Ochrony Danych Osobowych (Art 40). Na szczęście od tej zasady są liczne wyjątki (art 43 ustęp 1). M.in. z obowiązku rejestracji są zwolnieni administratorzy danych:

- przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,
- dotyczących osób należących do kościoła lub innego związku wyznaniowego, (...) przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego
- powszechnie dostępnych,
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

(wymieniono tylko najczęściej stosowane wyjątki!)

Należy jednak zwrócić uwagę że zwolnienie z obowiązku rejestracji zbioru danych w GIODO nie zwalnia z obowiązku przetwarzania ich zgodnie z wymogami Ustawy!

Po czwarte – Kto jest administratorem danych osobowych?

Art 7, ust. 4 Ustawy mówi że administrator danych to organ, jednostka organizacyjna, podmiot lub osoba, (...) decydujące o celach i środkach przetwarzania danych osobowych.

A więc w ogólnym przypadku można powiedzieć, że administratorem danych osobowych jest zarząd danej instytucji. Może to być zaskakujące dla osób, które nie miały wcześniej styczności z problematyką przetwarzania danych osobowych. W powszechnej świadomości funkcję administratora danych myli się z funkcją „administratora bezpieczeństwa informacji” (ABI), czyli osobą wyznaczoną do nadzorowania przestrzegania zasad ochrony danych osobowych (Art 36 ust 3). ABI jest odpowiedzialny przed zwierzchnikiem natomiast odpowiedzialnym z litery prawa jest instytucja (czyli w praktyce – jej zarząd).

## **Odpowiedzialność**

Art 49:

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Art 52:

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniami przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

### **Niektóre wymagania dotyczące baz danych**

Najogólniej wymagania dotyczące zabezpieczeń danych osobowych określa Art 36 ust. 1 ustawy, który mówi 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, zabraniami przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem”.

Precyzyjniejsze wymagania można znaleźć w towarzyszącym Ustawie Rozporządzeniu [2] oraz w dokumencie opublikowanym na stronie www GODO: „Wymagania dotyczące struktur baz danych (...)” [4]. Poniżej przedstawiam pokrótce najważniejsze wymagania których powinien być świadomy twórca i administrator baz danych i aplikacji, w których będą przetwarzane dane osobowe.

Podstawowym dokumentem określającym wymagania techniczne dotyczące systemów informatycznych jest Rozporządzenie MSWiA „w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych” [2]. W załączniku do tego rozporządzenia, są wymienione środki bezpieczeństwa jakie powinny być stosowane w systemie informatycznym przetwarzającym dane osobowe. Środki bezpieczeństwa zostały przypisane do trzech poziomów zabezpieczeń:

- podstawowy – dla wszystkich systemów,
- podwyższony – dla systemów przetwarzających dane o szczególnej wartości wymienione w Art. 27 ustawy (np. pochodzenie rasowe, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna lub związkowa, dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym, dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, itp.)
- wysoki - gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

Najważniejsze wymagania z punktu widzenia twórców i administratorów baz danych i aplikacji, sprecyzowane w Rozporządzeniu to:

- Konieczność stosowania mechanizmów kontroli dostępu, przy czym jeśli do systemu ma dostęp wielu użytkowników, to muszą mieć oni odrębne identyfikatory.

*Warto zwrócić uwagę na to, że jeśli by się ściśle trzymać tego zapisu, to z tego wymagania wynika pośrednio wymóg działania na osobnych kontach w bazie dla każdego użytkownika. Tzn, złą praktyką w przypadku przetwarzania danych osobowych, byłoby gdyby aplikacja działała na bazie danych zawsze na koncie*

*jednego użytkownika, niezależnie od użytkownika aplikacji (powszechnie stosowana praktyka w przypadku aplikacji webowych).*

- Zabezpieczenie przed „działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego” oraz „utrata danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej”.

*Zwracam uwagę że pierwsze z tych wymagań jest dość ogólne i pozostawia dużą dowolność interpretacji. Nie dotarłem też do żadnych dokumentów tłumaczących intencję ustawodawcy. Wypada przyjąć że w tym zakresie należy stosować zasady dobrej praktyki inżynierskiej czy też zalecenia producenta oprogramowania. W wypadku Oracle, mogą to być np. zalecenia z dokumentu „Secure Configuration Guide for Oracle9iR2” ([http://www.oracle.com/technology/deploy/security/oracle9i/pdf/9ir2\\_checklist.pdf](http://www.oracle.com/technology/deploy/security/oracle9i/pdf/9ir2_checklist.pdf)). Wiadomo, że nie ma systemów w 100% bezpiecznych, ale w razie kontroli lub co gorsza – w razie wycieku danych, warto jest móc dowiedzieć że dolożyło się wszelakich starań żeby właściwie zabezpieczyć dane (rozsądne byłoby np. przedstawienie wyników niezależnych ocen bezpieczeństwa i testów penetracyjnych).*

- Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
- Wymagania odnośnie haseł:
  - powinny być zmieniane nie rzadziej niż co 30 dni
  - hasło powinno się składać co najmniej:
    - na poziomie podstawowym: z 6 znaków,
    - na poziomie podwyższonym i wysokim: z 8 znaków i zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,

*Na poziomie bazy Oracle, wymagania te można wymusić za pomocą mechanizmu PROFILE.*

- Konieczność sporządzania kopii zapasowych danych i programów je przetwarzających (czyli należy wykonywać również backup samego oprogramowania DBMS). Ponadto kopie zapasowe należy przechowywać w „w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem” oraz usuwać niezwłocznie po ustaniu ich użyteczności.

*Ustawodawca nie reguluje już jednak częstotliwości sporządzania kopii zapasowych.*

- Jeśli dane są obecne na komputerze przenośnym to nakazane jest szyfrowanie danych.

*Można tu wykorzystać mechanizmy szyfrowania na poziomie bazy danych (np. DBMS\_OBFUSCATION\_TOOLKIT / DBMS\_CRYPTO) lub szyfrowanie plików lub całego filesystemu.*

- Urządzenia, dyski lub inne nośniki elektroniczne zawierające dane osobowe przeznaczone do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do przetwarzania danych osobowych (typowy przypadek – przekazanie starych komputerów szkole) pozbawia się wcześniej zapisu w sposób uniemożliwiający ich odzyskanie.

*Po sprawie słynnego dysku Jakubowskiej nie muszę chyba nikogo przekonywać, że sformatowanie dysku nie wypełnia powyższego warunku. Ustawodawca nie przekazał tutaj precyzyjniejszych wytycznych. Z technicznego punktu widzenia, zniszczenie zapisu w sposób uniemożliwiający odzyskanie danych, to kilkunastokrotne nadpisanie całości danych informacją losową. Powszechnie są dostępne programy wykonujące takie bezpieczne usuwanie danych z dysków. Innym sposobem jest rozmagnesowanie nośnika za pomocą specjalnego urządzenia.*

- Na poziomie wysokim należy stosować zabezpieczenia logiczne obejmujące:
  - „kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną”
  - „kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych”

*Wymagania te można zaimplementować stosując np. firewall, przy czym należy pamiętać o tym, że powinien on kontrolować również ruch wychodzący z systemu informatycznego.*

- Na poziomie wysokim należy zapewnić ochronę kryptograficzną wobec „danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej”.

*W większości wypadków, jeśli aplikacja udostępnia możliwość uwierzytelnienia z sieci publicznej, to jest to aplikacja webowa. W takim wypadku należy po prostu zastosować HTTPS (szyfrowanie SSL-em). Należy przy tym pamiętać o tym, żeby SSL był wdrożony zgodnie z zasadami dobrej praktyki (choćby Rozporządzenie nie wymaga tego wprost ;). Tu pozwolę sobie na małą uwagę na temat sensowności powyższego wymagania. Jest dla mnie niezrozumiałe dlaczego ustawodawca ograniczył się tylko i wyłącznie do konieczności szyfrowania danych uwierzytelniających (np. login/hasło). Jeśli będzie szyfrowane tylko hasło a dane będące wynikiem działania aplikacji będą przesyłane otwartym tekstem (tak jak jest to np. w protokole TNS charakterystycznym dla baz Oracle) to przecież intruz podsłuchujący dane i tak dopnie swego. Ponadto w przypadku aplikacji webowych, które chronią SSL-em tylko moment uwierzytelnienia a później „przełączają się” na zwykłe HTTP, bardzo łatwo można podsłuchać identyfikator sesji i podszyć się pod uwierzytelnionego użytkownika, bez konieczności poznania jego hasła.*

Z Podstawowego tekstu Ustawy również wynikają pewne wymagania dotyczące baz danych i aplikacji. Większość z nich została omówiona z praktycznego punktu widzenia w opracowaniu GODO pod tytułem „Wymagania dotyczące struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji” [4]. Dokument ten można znaleźć pod adresem: [http://www.giodo.gov.pl/plik/id\\_p/285/t/pdf/j/pl/](http://www.giodo.gov.pl/plik/id_p/285/t/pdf/j/pl/).

Najważniejsze wymagania techniczne omówione w tym dokumencie to:

- W aplikacji przetwarzającej dane osobowe powinna być dostępna opcja podglądu i weryfikacji przetwarzanych danych osobowych. Ponieważ wymóg ten wynika z zapisu Ustawy, który mówi o prawie dostępu osoby do treści jej danych osobowych, to wymagane jest również żeby dane te były wyświetlane i drukowane w postaci zrozumiałej dla przeciętnej odbiorcy. Ważne jest

- również to, że funkcja wyświetlania/wydruku powinna działać w ten sposób żeby wyświetlać dane tylko i wyłącznie jednej osoby. GIODO zwraca uwagę na to, że zapytanie do bazy danych obsługujące tą funkcję powinno być skonstruowane w ten sposób, żeby zwracać dane tylko jednej wyszukiwanej osoby.
- Ustawa często posługuje się terminem „zrozumiałe dla przeciętnego odbiorcy”. W tym zakresie wytyczne GIODO zwracają uwagę na to że na wydruku lub formatce opisy pól i same dane były prezentowane w pełnym brzmieniu a nie w postaci kodowanej lub zapisanej skrótowo.
  - Rekordy z danymi osobowymi usuwane z bazy powinny być kasowane w rzeczywistości a nie zaznaczane jako skasowane. Tak żeby odpowiednie programy narzędziowe nie mogły tych danych odzyskać.  
*Znowu – jeśliby wprost interpretować ten przepis, to należałoby również uwzględnić kopie danych w postaci: kopii zapasowych, redo logów, plików trace, danych flashback query i innych miejsc z których dane mogłyby być odzyskane.*
  - Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne.  
W praktyce ten zapis Ustawy oznacza że indeksy nie mogą zawierać znaczeń ukrytych. W większości przypadków tak jest, ale warto zwrócić uwagę na to żeby sposób tworzenia indeksów (np. „standardowy mechanizm Oracle”) opisać w dokumentacji, dla uniknięcia niejasności w razie ewentualnej kontroli.
  - Aplikacja i baza danych powinny umożliwiać wyświetlenie/wydrukowanie dla danej osoby raportu, w którym będą uwzględnione: przetwarzane dane tej osoby, źródło z którego pochodzą dane jej dotyczące, kto dopisał te dane (operator), data/czas utworzenia, informacje o modyfikacjach (kto, kiedy), informacje o tym komu, kiedy i w jakim zakresie dane były udostępniane. Przykład właściwej formy takiego raportu znajduje się w dokumencie [4].

Jak widać, przetwarzanie danych osobowych w systemach informatycznych wiąże się z przestrzeganiem wielu zaleceń technicznych. Aplikacja która do tego służy powinna posiadać odpowiednie funkcje wynikające z ustawy, a baza danych – odpowiednią organizację danych. Powyżej wymieniono jedynie główne wymagania techniczne dotyczące aplikacji i baz danych. Ustawa i Rozporządzenie zawierają więcej wymogów, które mają zastosowanie w specyficznych sytuacjach. Ponadto poza wymogami technicznymi, administrator danych osobowych powinien również spełnić inne wymagania wynikające z Ustawy. Do najważniejszych należy zaliczyć wymóg udokumentowania systemu, w tym posiadanie polityki i instrukcji bezpieczeństwa (patrz wytyczne GIODO [5] i [6]).

## **Bibliografia**

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.)
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać

- urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (Dz. U. z 2004 r. Nr 100, poz. 1024)
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 100, poz. 1025)
  4. Wymagania dotyczące struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji ([http://www.giodo.gov.pl/plik/id\\_p/285/t/pdf/j/pl/](http://www.giodo.gov.pl/plik/id_p/285/t/pdf/j/pl/))
  5. Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa ([http://www.giodo.gov.pl/plik/id\\_p/551/t/pdf/j/pl/](http://www.giodo.gov.pl/plik/id_p/551/t/pdf/j/pl/))
  6. Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. ([http://www.giodo.gov.pl/plik/id\\_p/550/t/pdf/j/pl/](http://www.giodo.gov.pl/plik/id_p/550/t/pdf/j/pl/))
  7. Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych z działalności za rok 2003.
  8. Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych z działalności za rok 2002.
  9. UODO Survival Kit - ISACA Warsaw Chapter (<http://www.isaca.org.pl/projects/WCP9/index.html>)
  10. Privacy Protections in Oracle Database 10g – An Oracle Whitepaper ([http://www.oracle.com/technology/ deploy/security/db\\_security/pdf/privacy10g.pdf](http://www.oracle.com/technology/ deploy/security/db_security/pdf/privacy10g.pdf))