Wymagania dotyczące struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji

(w świetle ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.
- t. j. Dz. U. z 2002 r. Nr 101, poz. 926, z pózn. zm.)

Ustawa o ochronie danych osobowych określa nie tylko prawa osoby do ochrony jego danych, ale precyzuje również szereg wymagań w stosunku do wszystkich podmiotów, które danymi takimi dysponują.

Art. 24. ust. 1. **pkt. 3** ustawy wymaga, aby administrator danych informował osobę, której dane zostają umieszczone w zbiorze danych, **o prawie dostępu do treści danych tej osoby oraz prawie do ich poprawiania**,

W odniesieniu do aplikacji zarządzającej przetwarzaniem danych osobowych realizacja wskazanego obowiązku wymaga, aby z poziomu aplikacji dostępna była specjalna opcja podglądu i weryfikacji przetwarzanych danych osobowych. Opcja taka powinna umożliwiać: a) jednoznaczną identyfikację danych osobowych wskazanej osoby, b) wyświetlenie oraz wydruk przetwarzanych danych w postaci zrozumiałej dla przeciętnego odbiorcy, c) korektę przetwarzanych danych. Ta ostatnia funkcja powinna być dostępna tylko dla osób uprawnionych do zmiany przetwarzanych danych.

Wymóg dotyczący jednoznacznej identyfikacji danych osobowych przetwarzanych w zbiorze wynika z konieczności ograniczenia zainteresowanej osobie dostępu tylko do tych danych, które jej dotyczą. Osoba, której dane przetwarzane są w systemie informatycznym ma jedynie prawo do przeglądania i żądania zmiany tylko tych danych, które jej dotyczą. Funkcja służąca zatem do podglądu danych osobowych przetwarzanych w systemie informatycznym, jeżeli podgląd ten przewiduje się wykonywać w obecności osób, które życzą sobie dostępu do swoich danych, powinna być tak skonstruowana, aby na monitorze nie zostały przypadkowo wyświetlone dane innych osób. Aby niebezpieczeństwo takie wyeliminować, konstrukcja zapytań do zbioru przetwarzanych danych powinna zapewnić jednoznaczną identyfikację wyszukiwanej osoby. Oznacza to, że odpowiedzią na zapytanie wyszukania danych powinno być udostępnione danych tylko jednej, wyszukiwanej właśnie osoby. Niedopuszczalne jest, aby w obecności np. Jana Kowalskiego nr 1, na ekranie komputera w wyniku zapytania o jego dane wyświetlone zostały dane innych osób o tym samym nazwisku (patrz również art. 36 ustawy). Rozwiązanie takie, tzw. przybliżone wyszukiwanie, jest dopuszczalne tylko wtedy,

gdy wyniki wyszukiwania są dostępne wyłącznie dla osób upoważnionych do przetwarzania danych osobowych.

W **art. 26 ust. 1 pkt. 4** ustawy ustawodawca nakazuje, aby administrator danych dołożył szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. W szczególności chodzi tutaj o to, aby dane osobowe były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Realizacja powyższego obowiązku wymaga od aplikacji przetwarzającej dane osobowe, aby jednoznacznie realizowany był wymóg "usunięcia danych" ze zbioru (bazy danych). Chodzi tutaj głównie o to, aby opcja realizująca usuwanie pozycji ze zbioru polegała na **rzeczywistym ich usunięciu lub nadpisaniu** informacją pustą, a nie zaznaczeniu danego rekordu, jako rekordu skasowanego, który staje się często jedynie niewidocznym z poziomu aplikacji, ale dalej istnieje w przetwarzanym zbiorze danych. W tym ostatnim przypadku jest możliwość, przy użyciu odpowiednich programów narzędziowych, ponownego "odkrycia" usuniętego w ten sposób zapisu danych i dalszego ich przetwarzania. Rzeczywiste usunięcie lub nadpisanie informacją "pustą" kasowanych danych uniemożliwia dokonywanie jakichkolwiek dalszych modyfikacji na tych danych.

Szczególną uwagę projektanci aplikacji zarządzających bazami danych osobowych powinni zwrócić również na **art. 28. ust. 2 i 3** ustawy, który brzmi:

2. **Numery porządkowe stosowane w ewidencji ludności mogą zawierać tylko oznaczenia płci, daty urodzenia, numer nadania oraz liczbę kontrolną.**
3. Zabronione jest nadawanie **ukrytych znaczeń** elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne.

Wymagania dotyczące zawartości tych pól informacyjnych w zbiorach danych osobowych, w których przechowywane są numery porządkowe (indeksy) zakazują ich wykorzystywania do kodowania innych wartości niż płeć, data urodzenia, numer pozycji w rejestrze oraz liczba kontrolna. Wymagania te odnoszą się nie tylko do pól informacyjnych w zbiorach danych osobowych, ale również do zawartości kolumn w tablicach SQL-owych baz danych, w których przechowywane są dane osobowe. Cytowany przepis zakazuje nadawanie takim polom jakichkolwiek innych ukrytych znaczeń. W dokumentacji systemu zarządzania bazą danych osobowych, sposób tworzenia numerów porządkowych i/lub indeksów, jeśli nie są to kolejne liczby naturalne określające pozycję zapisu w zbiorze, powinien być dokładnie

opisany i wyjaśniony. Wyjaśnienie takie jest niezbędne w celu wykazania, że dany system przetwarzania danych osobowych spełnia wskazane wymagania.

Odpowiedniej struktury bazy danych oraz specjalnych opcji użytkowych od systemu informatycznego przetwarzającego dane osobowe wymaga również realizacja przepisów ustawy zawartych w art. 32 ust. 1 pkt. 3, pkt. 4, pkt. 5 i art. 33, których brzmienie jest następujące:

Art. 32 ust. 1.

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

3. **uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,**
4. uzyskania informacji o **źródle, z którego pochodzą dane jej dotyczące,** chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,
5. uzyskania informacji o **sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,**

Art. 33 ust.1 pkt. 4

Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt. 1 – 5a, a w szczególności podać w formie zrozumiałej w jakim zakresie oraz komu dane zostały udostępnione.

Art. 32 ust. 1 pkt. 5 w powiązaniu z §7 ust. 1 pkt. 4 rozporządzenia, stawia w odniesieniu do struktury bazy danych oraz aplikacji zarządzającej zbiorem danych osobowych wymaganie posiadania opcji umożliwiającej rejestrację daty, zakresu i sposobu udostępniania danych **odbiorcom** (w myśl art. 6 pkt. 7 ustawy), jeśli konieczność takiego udostępnienia wynika z przepisów prawa lub jest przewidziana przez administratora danych. Informacje dotyczące udostępnienia powinny być rejestrowane w taki sposób, aby dla każdej osoby, której dane są zawarte w zbiorze, możliwe było ich odczytanie i sporządzenie stosownego raportu (art. 33 ust. 1 pkt. 4 ustawy). Oznacza to, że pola informacyjne przeznaczone do wpisania udostępnień powinny być w strukturze zbioru danych powiązane relacją przyporządkowania wskazującą osobę, której dotyczą. Należy przy tym pamiętać, że dane przetwarzane w zbiorze dotyczące danej osoby mogą być udostępnione wielu różnym podmiotom, w różnych

okresach czasu. Stąd też niezbędne jest opracowanie takiej struktury zbioru danych, która umożliwi odnotowywanie wielu udostępnień danych odnoszących się do tej samej osoby. W przypadku, gdy ten sam podzielony funkcjonalnie zbiór przetwarzany jest w co najmniej dwóch różnych systemach informatycznych, zgodnie z §7 ust. 4 rozporządzenia, odnotowanie informacji o udostępnieniu danych odbiorcom może być realizowane w jednym z tych systemów lub w systemie trzecim dedykowanym wyłącznie temu celowi. Natomiast w przypadku, gdy mamy do czynienia z różnymi zbiorami, jakimi są np. zbiór klientów i zbiór pracowników, przetwarzanymi w różnych systemach informatycznych, odnotowanie, o którym mowa powyżej należy realizować w każdym z tych systemów lub w odrębnym systemie dedykowanym temu celowi.

Istotnym warunkiem zgodności aplikacji przetwarzających dane osobowe z ustawą o ochronie danych osobowych jest również posiadanie funkcjonalności umożliwiającej wyświetlenie oraz wydruk danych osobowych w postaci umożliwiającej łatwe i jednoznaczne zrozumienie ich treści (§7 pkt. 3 rozporządzenia). Oznacza to, że poszczególne dane powinny być prezentowane w pełnym brzmieniu, poprzedzone nazwą opisową danego pola, to jest nazwą, której znaczenie jest powszechnie zrozumiałe jak np. na rys. 1 lub 2. Przykładowy zestaw takich danych przedstawiono w części A poniżej zamieszczonej tabeli.

A - Informacje identyfikujące osobę	
Nazwa danej	**Wartość**
Pierwsze imię	Jan
Drugie imię	Zygmunt
Nazwisko	Kowalski
Ulica, nr domu i mieszkania	Nalewki 20 m.10
Kod pocztowy	00-701
Miejscowość	Warszawa
Data urodzenia	12 listopad 1954
PESEL	54111203431
B - Informacje z zakresu § 7 ust. 1 pkt. 1, 2, 3, 5 rozporządzenia	
Nazwa danej	**Wartość**
data 1-szego wprowadzenia danych do systemu	12.10.1999
źródło pochodzenia danych	od osoby, której dotyczą
Identyfikator użytkownika wprowadzającego dane	a_grzeskowiak
zgoda na przetwarzanie danych	Tak

zgoda na przetwarzanie danych w celach marketingowych	Nie

C - Informacje o udostępnieniach § 7 ust. 1 pkt. 4 rozporządzenia

L.p.	Nazwa i adres podmiotu, któremu przekazano dane	Data udostępnienia	Zakres udostępnionych danych
1	Firma "ABC" S.A. ul. Pańska 4 00-920 Wrocław	30.11.2000	• imię i nazwisko • adres zamieszkania • PESEL • imię ojca
2	Firma “XYZ” Sp. z o.o. ul. Puławska 7 00-600 Warszawa	17.08.2000	• imię i nazwisko • adres zamieszkania • PESEL
...	...	...	...
N	...	...	...

Rys. 1 Przykład właściwej formy raportu zawierającego informacje, o których mowa w §7 ust. 1 rozporządzenia

W przypadku gdy dane osobowe prezentowane są w postaci zredagowanej formatki jak na rys. 2, wówczas kolejne jej pola informacyjne powinny być jednoznacznie oznaczone, tak jak zostało to zaprezentowane na poniższym przykładzie.

Imię (imiona):	**Jan Zygmunt**	Nazwisko:	**Kowalski**
Adres:	**Nalewki 20 m. 10;**	Imię ojca:	**Grzegorz**
	00-701 Warszawa		
Data urodzenia:	**12 listopad 1954**	Imię matki:	**Katarzyna**
Nr PESEL:	**6711203221**	Miejsce pracy:	**“Zygfryt” S.A.;**
Wykształcenie:	**wyższe**		**Ul. Korty 10,**
			Płocko

Rys. 2 Sposób poprawnej prezentacji danych przetwarzanych w systemie informatycznym

Opcja prezentacji danych nie powinna wyświetlać/drukować danych w postaci kodów, jakie często są stosowane w wewnętrznej strukturze bazy danych w celu jej optymalizacji lub normalizacji wewnętrznej struktury danych (Rys. 3).

Jeżeli np. w strukturze bazy istnieje słownik kodów wykształcenia w postaci:

w – wyższe,

s – średnie,

z – zawodowe,

oraz w strukturze zapisu danych i ewentualnie innych procedurach przetwarzania operuje się nie pełnym opisem wartości danych, lecz wprowadzonymi kodami, to jednak, niezależnie od tego, podczas ich prezentacji, należy przedstawić ich pełne opisy. Opisy te nie powinny być wieloznaczne. Nie należy w tym celu używać skrótów, których znaczenie w przypadku braku wystarczającego kontekstu mogłoby budzić wątpliwości, jak np. użycie skrótu "*arch*." dla oznaczenia zawodu *architekt*, który może być interpretowany również jako skrót słowa *archiwista* lub *archeolog*.

Imię (imiona):	**Jan Zygmunt**	Nazwisko:	**Kowalski**
Adres:	**Nalewki 20 m. 10;**	Imię ojca:	**Grzegorz**
	00-701 Warszawa		
Data urodzenia:	**12 listopad 1954**	Imię matki:	**Katarzyna**
Nr PESEL:	**6711203221**		
		Miejsce pracy:	**"Zygfryt" S.A.**
Wykształcenie:	**W**		

Rys. 3 Przykład nieprawidłowego sposobu prezentacji danych osobowych w systemie informatycznym

Odpowiedniej struktury bazy danych oraz specjalnych opcji użytkowych od systemu informatycznego przetwarzającego dane osobowe wymaga również realizacja obowiązku, o którym mowa w **art. 38**, którego brzmienie jest następujące: administrator danych przetwarzanych w systemie informatycznym jest obowiązany **zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,** zwłaszcza, gdy przekazuje się je za pomocą urządzeń teletransmisji danych.

Art. 38 ustawy poza przedstawionymi już wyżej wymogami dotyczącymi rejestracji zdarzeń dotyczących udostępniania danych innym podmiotom, określa również wymagania dotyczące rejestracji danych związanych z wewnętrzną organizacją przetwarzania. Do danych takich należą między innymi informacje o dacie wprowadzenia danych do systemu oraz osobie, która je wprowadziła. System informatyczny służący do przetwarzania danych osobowych powinien, więc posiadać własności, które zapewniają odpowiednią **autoryzację i**

rozliczalność przetwarzanych danych. Przez autoryzację należy tu rozumieć właściwość zapewniającą, że dostęp do systemu informatycznego uzyskują jedynie osoby, które posiadają odpowiednie upoważnienie i zostały w tym systemie zarejestrowane. Przez rozliczalność zaś, należy rozumieć własność zapewniającą możliwość jednoznacznego wskazania osoby, która określone dane do systemu wprowadziła lub zmieniła. Ponadto, rozliczalność przetwarzania danych osobowych w systemie informatycznym powinna zapewniać również możliwość ustalenia daty wprowadzania danych osobowych do systemu.

Data aktualizacji: 05.11.2004 r.