

DOBRE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH ZAKŁADÓW UBEZPIECZEŃ

Andrzej Kaczmarek

BIURO

GENERALNEGO INSPEKTORA OCHRONY
DANYCH OSOBOWYCH

11. 05. 2009 r. Warszawa

DOBRE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH ZAKŁADÓW UBEZPIECZEŃ



PLAN

- ✓ **Podstawy prawne przetwarzania danych osobowych w działalności ubezpieczeniowej**
- ✓ **Przetwarzanie danych osobowych w na etapie werbowania klientów i zawierania umów**
- ✓ **Przetwarzanie danych osobowych na etapie likwidacji szkód**
- ✓ **Polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi**

PODSTAWY PRAWNE (PRZEPISY OGÓLNE)

- **Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)**
- **Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144 poz. 1204 z późn. zm.)**
- **Ustawa z dnia 22 maja 2003 r. o działalności ubezpieczeniowej tj. (Dz. U. z 2010 r. Nr 11, poz. 66, ze zm.)**
- **Ustawa z dnia 22 maja 2003 r. o pośrednictwie ubezpieczeniowym (Dz. U. Nr 124, poz. 1154, z późn. zm.)**
- **Ustawa z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz. U. Nr 124, poz. 1152, z późn. zm.)**

PODSTAWY PRAWNE (PRZEPISY SZCZEGÓŁOWE)

- **Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (tj. Dz. U. z 2007 r. Nr 11 poz. 74 z późn. zm.**
- **Ustawa z dnia 20 grudnia 1990 r. o ubezpieczeniach społecznych rolników (t.j. Dz. U. z 2008 r. Nr 50 poz. 291 ze zm.)**
- **Ustawa z dnia 17 grudnia o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (tj. Dz. U z 2004 r. Nr 39 poz. 353 z późn. zm.)**
- **INNE**

ZASADY PRZETWARZANIA DANYCH (1)

Przetwarzanie danych na etapie zawierania umowy oraz poprzedzającym jej zawieranie

- **źródła pozyskiwania danych (legalność);**
- **sposoby pozyskiwania danych (obowiązek informacyjny, bezpieczeństwo);**
- **okres przetwarzania danych (warunki dalszego przetwarzania jeśli umowa nie zostanie zawarta);**
- **wymiana danych (przesłanki).**

ZASADY PRZETWARZANIA DANYCH (2)

Przetwarzanie danych po zawarciu umowy

- **zakres przetwarzania danych (zależny od rodzaju ubezpieczenia);**
- **zapewnienie kontroli nad tym komu, gdzie, kiedy i jakie dane zostały do zbioru wprowadzone oraz komu są przekazywane;**
- **rejestr informacji o udostępnieniach danych odbiorcom (kto jest odbiorcą danych?) – art.. 19 ust. 2 u.o.d.u.**
 - ✓ **Wymiana danych w związku z działaniami odszkodowawczymi.**
 - ✓ **Wymiana danych w związku z działaniami mającymi na celu zapobieganie przestępczości ubezpieczeniowej.**

REALIZACJA OBOWIĄZKU INFORMACYJNEGO (1)

W ramach obowiązku informacyjnego zgodnie z art. 24 i 25 u.o.d.o. należy informować o:

- **Administratorze danych tj. o tym, kto jest administratorem danych (nazwie i siedzibie podmiotu).**
- **Celu przetwarzania danych a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,.**
- **Zakresie przetwarzanych danych.**
- **Prawie dostępu do treści swoich danych oraz ich poprawiania.**
- **Dobrowolności albo obowiązku podania danych, a jeśli taki obowiązek istnieje, o jego podstawie prawnej.**
- **Prawach wynikających z art. 32 u.o.d.o**

REALIZACJA OBOWIĄZKU INFORMACYJNEGO (2)

W przypadku wykorzystywania systemu informatycznego do pozyskiwania danych dodatkowo należy spełnić obowiązek informacyjny w sposób wynikające z art. 5 u.ś.u.d.o. poprzez podanie:

- adresu elektronicznego administratora danych;**
- imienia, nazwiska, miejsca zamieszkania i adresu albo nazwy lub firmy oraz siedziby i adresu;**
- informacji dotyczących właściwego zezwolenia (jeśli takie jest wymagane);**
- jeśli usługodawca jest osobą fizyczną, której prawo do wykonywania zawodu jest uzależnione od spełnienia określonych w odrębnych ustawach wymagań, podaje również te inne wymagane informacje.**

REALIZACJA OBOWIĄZKU INFORMACYJNEGO (3)

Zgodnie z art. 32 u.o.d.o. osobie, której dane są przetwarzane przysługuje prawo do

- ✓ **uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;**
- ✓ **uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące;**
- ✓ **uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;**
- ✓ **uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2.**

JAK PRAWA OSÓB I OBOWIĄZKI ADMINISTRATORA PRZEKŁADAJĄ SIĘ NA FUNKCJONALNOŚĆ SYSTEMÓW IT

**System informatyczny powinien zapewniać
możliwość odnotowania informacji o:**

- ✓ nazwie i siedzibie administratora danych;
- ✓ celach i zakresie zbieranych danych;
- ✓ źródle /źródłach pozyskania danych;
- ✓ użytkownikach systemu, którzy dane wprowadzili;
- ✓ dacie wprowadzenia danych;
- ✓ udostępnieniach danych w zakresie kiedy, jakie dane, komu i w jakim celu zostały udostępnione;
- ✓ zgłoszeniach sprzeciwu wobec przetwarzania danych.

JAK OBOWIĄZKI ADMINISTRATORA PRZEKŁADAJĄ SIĘ NA BEZPIECZEŃSTWO SYSTEMÓW IT (1)

System informatyczny używany do przetwarzania danych powinien:

- ✓ **umożliwić dostęp do danych tylko osobom posiadającym stosowne upoważnienia;**
- ✓ **zapewniać rozliczalność i integralność wykonywanych operacji;**
- ✓ **być odpornym na zagrożenia pochodzące z sieci wewnętrznej jak i zewnętrznej;**
- ✓ **zapewniać poufność danych przekazywanych poprzez sieć publiczną;**
- ✓ **zapewniać możliwość weryfikacji administratora poprzez system certyfikacji.**

ZGODNOŚĆ Z KRAJOWYMI ORAZ MIĘDZYNARODOWYMI STANDARDAMI

Zadania w zakresie funkcjonalności i bezpieczeństwa systemów IT powinny być na każdym etapie realizowane z wykorzystaniem stosownych standardów.

- ✓ **PN-ISO/IEC 17799:2007 (ISO 27002) - praktyczne zasady zarządzania bezpieczeństwem informacji;**
- ✓ **PN-ISO/IEC 27001:2007 (PN-I-07799-2:2005) – specyfikacja systemów zarządzania bezpieczeństwem informacji;**
- ✓ **PN-ISO/IEC 27005 – Zarządzanie ryzykiem bezpieczeństwa informacji.**

NAJCZĘŚCIEJ SPOTYKANE UCHYBIENIA

- ✓ **nieprawidłowe wykonanie obowiązku informacyjnego;**
- ✓ **niewłaściwe zabezpieczenie teletransmisji i/lub możliwości weryfikacji administratora systemu;**
- ✓ **niewłaściwa realizacja wymagań funkcjonalnych w zakresie realizacji odnotowywania udostępnień;**
- ✓ **brak lub niekompletna dokumentacja procesu przetwarzania danych (polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym);**
- ✓ **niewłaściwe zarządzanie systemem bezpieczeństwa, brak lub niekompletne umowy powierzenia przetwarzania danych innym podmiotom.**

ZŁE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

PRZYKŁADY (1)

Brak informacji o administratorze strony (systemu IT)

OFEdlaCiebie.pl

Ranking OFE Aviva Generali ING PZU Zapisz się

Niezbędnik:

- RANKING OFE
- Czym jest system emerytalny?
- Co daje wybór dobrego OFE?
- OFE po raz pierwszy
- Zmiana OFE
- Aktualności
- DARMOWY Kurs e-mailowy
- Blog eksperta OFEdlaCiebie.pl
- Kontakt - napisz do nas

Zapisy online:

- ***WYPEŁNIJ FORMULARZ***
- Jak to się odbywa?
- Rekomendacje

Zastanawiasz się: "Jaki Fundusz Emerytalny wybrać...?"

Wybierz w oparciu o wiarygodny ranking OFE.

Oni już wiedzą, które Fundusze Emerytalne są najlepsze. Teraz Twoja kolej...

Ranking OFE 2010

W naszej analizie bazujemy na 4 bardzo solidnych i uznanych źródłach informacji:
1. Komisji Nadzoru Finansowego (3-letnie stopy zwrotu oraz od początku działalności)

PRZYKŁADY (2)

Sprzeczne dane dotyczące zabezpieczenia transmisji

Wybierając OFE za pośrednictwem OFEdlaCiebie.pl zyskujesz:

- bezpieczeństwo, minimum formalności i oszczędność czasu,
- satysfakcję z samodzielnego podjęcia decyzji w oparciu o niezależne rankingi OFE (bez zbędnych nerwów i spotkań z akwizytorami OFE),
- PAMIĘTAJ z OFEdlaCiebie.pl przystępujesz do Funduszu Emerytalnego bezpłatnie oraz kontrolujesz wyniki wybranego OFE!

W razie jakichkolwiek pytań służymy pomocą - [kontakt](#)

WYPEŁNIJ FORMULARZ TERAZ!

Przesyłane dane są bezpieczne!

Formularz jest szyfrowany

Wybieram: *

Fundusz Emerytalny: *

Dane członka Funduszu:

Nazwisko *

Pierwsze Imię *

Drugie Imię

Data urodzenia

PESEL *

NIP *

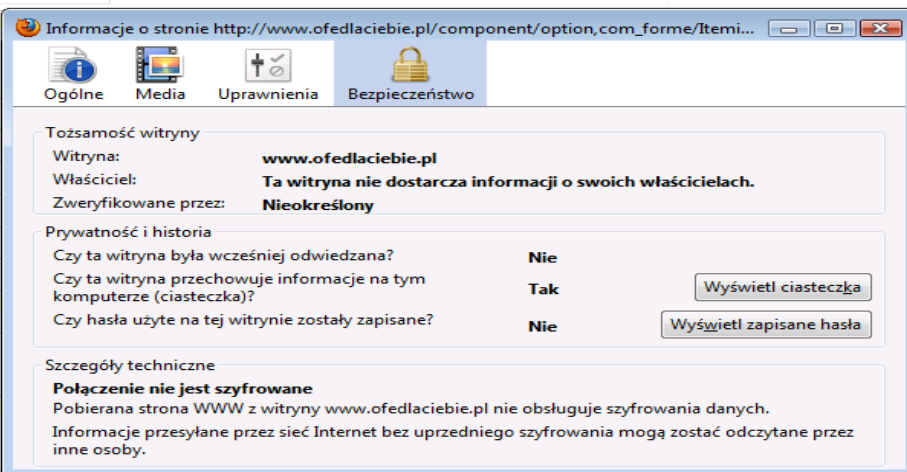
Dokument tożsamości *

Seria i numer dokumentu tożsamości

Stan cywilny: *

Adres zameldowania

Ulica:



Informacje o stronie http://www.ofedlaciebie.pl/component/option,com_forme/Itemid...

Ogólne Media Uprawnienia **Bezpieczeństwo**

Tożsamość witryny
Witryna: **www.ofedlaciebie.pl**
Właściciel: **Ta witryna nie dostarcza informacji o swoich właścicielach.**
Zweryfikowane przez: **Nieokreślony**

Prywatność i historia
Czy ta witryna była wcześniej odwiedzana? **Nie**
Czy ta witryna przechowuje informacje na tym komputerze (ciasteczka)? **Tak**
Czy hasła użyte na tej witrynie zostały zapisane? **Nie**

Szczegóły techniczne
Połączenie nie jest szyfrowane
Pobierana strona WWW z witryny www.ofedlaciebie.pl nie obsługuje szyfrowania danych.
Informacje przesyłane przez sieć Internet bez uprzedniego szyfrowania mogą zostać odczytane przez inne osoby.

PRZYKŁADY (3)

Nieprawidłowe informacje o celu przetwarzania

Wybierz produkt | Twoje potrzeby | Serwis Klienta | Serwis finansowy | O firmie | Kontakt

ING > Kontakt OFE

Wyślij wiadomość

Teraz możesz przystąpić do OFE bez wychodzenia z domu!

[Wypełnij deklarację OFE on-line \(ok. 10 min\)](#)

lub

prześlij nam dane kontaktowe, resztę załatwimy za Ciebie! (ok. 10 sek)

Podaj swoje dane:

Imię i nazwisko:*	<input type="text" value="Andrzej Kaczmarek"/>
Miejscowość:*	<input type="text" value="Warszawa"/>
Kod pocztowy:*	<input type="text" value="02-797"/>
Telefon:*	<input type="text" value="601 805082"/>
E-mail:*	<input type="text" value="andrzej.kaczmarek@acn.waw.pl"/>

Podanie powyższych danych jest dobrowolne. Administratorem Pana/Pani danych osobowych jest ING Otwarty Fundusz Emerytalny z siedzibą w Warszawie, przy ul. Ludnej 2. Pana/Pani dane osobowe będą przetwarzane wyłącznie w celu udzielenia odpowiedzi na pytania zawarte na niniejszym formularzu. Przysługuje Panu/Pani prawo dostępu do treści swoich danych osobowych oraz prawo ich poprawiania.

* pole obowiązkowe

[Powrót](#)

Centrum Obsługi Telefonicznej 0 801 20 30 40 | Bezpieczeństwo | Regulamin | Kontakt | Mapa Serwisu | ing.pl © 2008 ING. Wszelkie prawa zastrzeżone.

Kontakt

- Wyślij wiadomość
- Zadzwoń: 0 801 20 30 40
z komórki: (022) 522 71 24
- Znajdź Placówkę

Ubezpiecz życie

Ubezpiecz życie

Polecamy

- Przystąp do OFE on-line
- Ile może wynieść Twoja emerytura?
- portalemerytalny.pl
- Notowania UFK
- Stopy zwrotu OFE
- Formularze zmian
- Informacje na temat wypłaty świadczeń
- Polecenie zapłaty

Logowanie

ZŁE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

PRZYKŁADY (4) Nieprawidłowo wykonany obowiązek informacyjny

WYPEŁNIJ FORMULARZ TERAZ! - Fundusze Emerytalne-Ranking Funduszy Emerytalnych-OFEdlaCie...

http://www.ofedlaciebie.pl

Plik Edycja Widok Ulubione Narzędzia Pomoc

Ulubione WYPEŁNIJ FORMULARZ TERAZ! - Fundusze Emer...

- bezpieczeństwo, minimum formalności i oszczędność czasu,
- satysfakcję z samodzielnego podjęcia decyzji w oparciu o niezależne rankingi OFE (bez zbędnych nerwów i spotkań z akwizytorami OFE),
- PAMIĘTAJ z OFEdlaCiebie.pl przystępujesz do Funduszu Emerytalnego bezpłatnie oraz kontrolujesz wyniki wybranego OFE!

W razie jakichkolwiek pytań służymy pomocą - [kontakt](#)

WYPEŁNIJ FORMULARZ TERAZ!

Przesyłane dane są bezpieczne!

Formularz jest szyfrowany

Wybieram: *

Fundusz Emerytalny: *

Dane członka Funduszu:

Nazwisko *

Pierwsze Imię *

Kod pocztowy:

Miejscowość:

Gmina:

Wyrażam zgodę na wykorzystanie moich danych osobowych podanych w niniejszym formularzu, w celu zawarcia umowy przystąpienia do wybranego otwartego funduszu emerytalnego.

Wyślij Formularz

**DOBRE PRAKTYKI PRZETWARZANIA DANYCH
OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH
ZAKŁADÓW UBEZPIECZEŃ**



Dziękuję za uwagę!

Andrzej Kaczmarek

email: A_Kaczmarek@giodo.gov.pl

www.giodo.gov.pl