DOBRE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH ZAKŁADÓW UBEZPIECZEŃ

Andrzej Kaczmarek

BIURO
GENERALNEGO INSPEKTORA OCHRONY
DANYCH OSOBOWYCH

11. 05. 2009 r. Warszawa

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

DOBRE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH ZAKŁDÓW UBEZPIECZEŃ

GIODO
Generalny Inspektor Ochrony Danych Osobowych

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**

GIODO
Generalny Inspektor Ochrony Danych Osobowych

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**

GIODO
Generalny Inspektor Ochrony Danych Osobowych

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 STSTEMÓW 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 STSTEMÓW 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.**

ZŁE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

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)

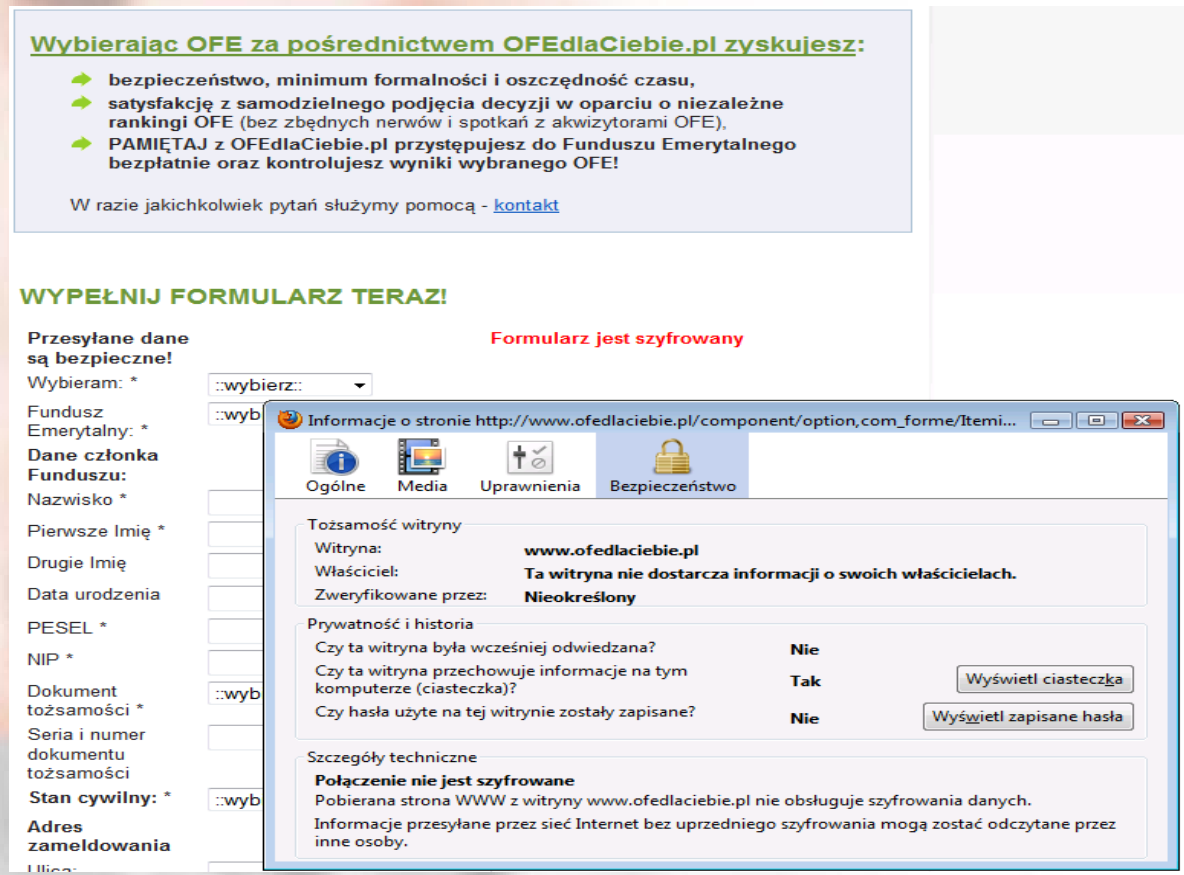
Brak informacji o administratorze strony (systemu IT)

ZŁE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

PRZYKŁADY (2)

Sprzeczne dane dotyczące zabezpieczenia transmisji

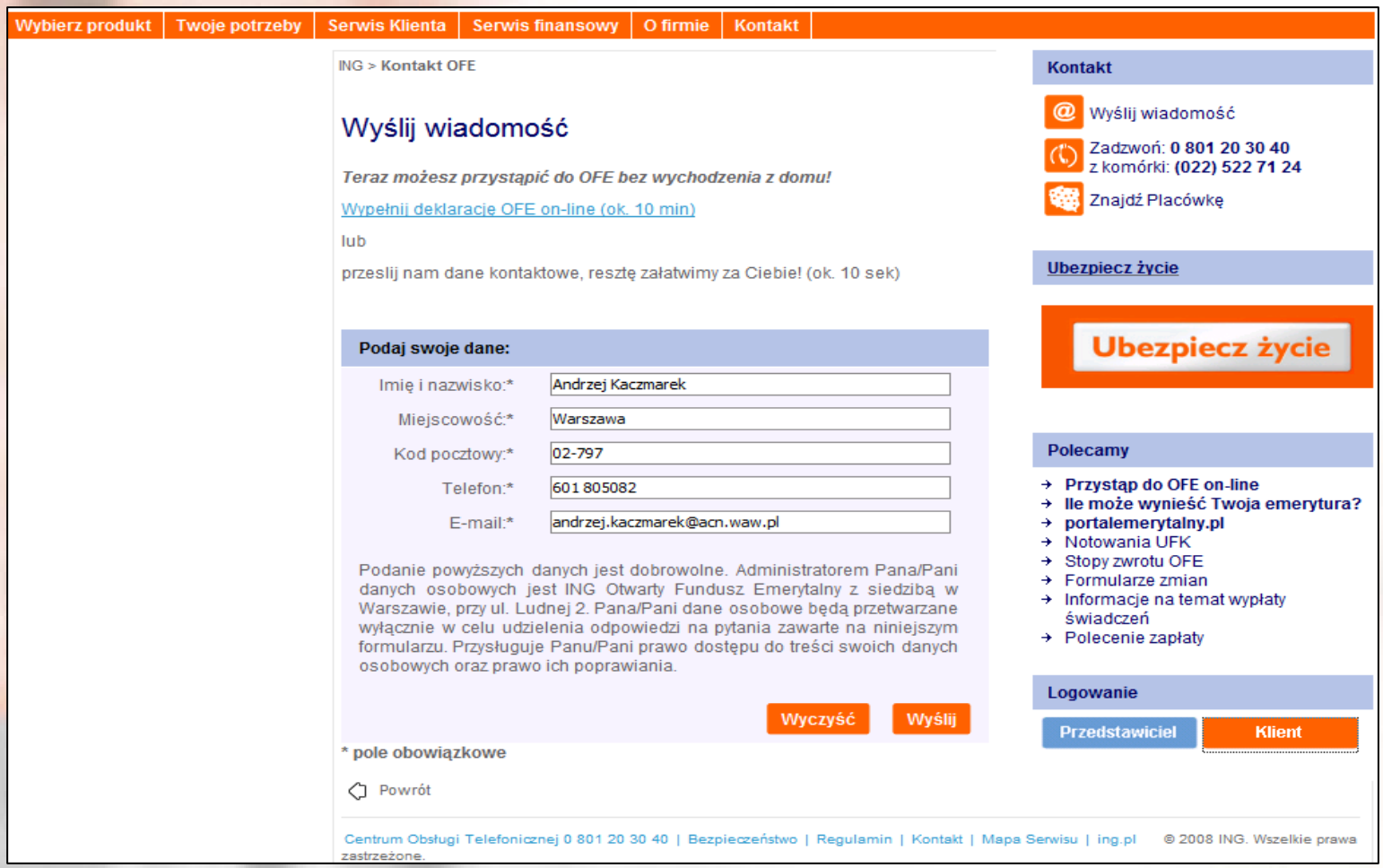


ZŁE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

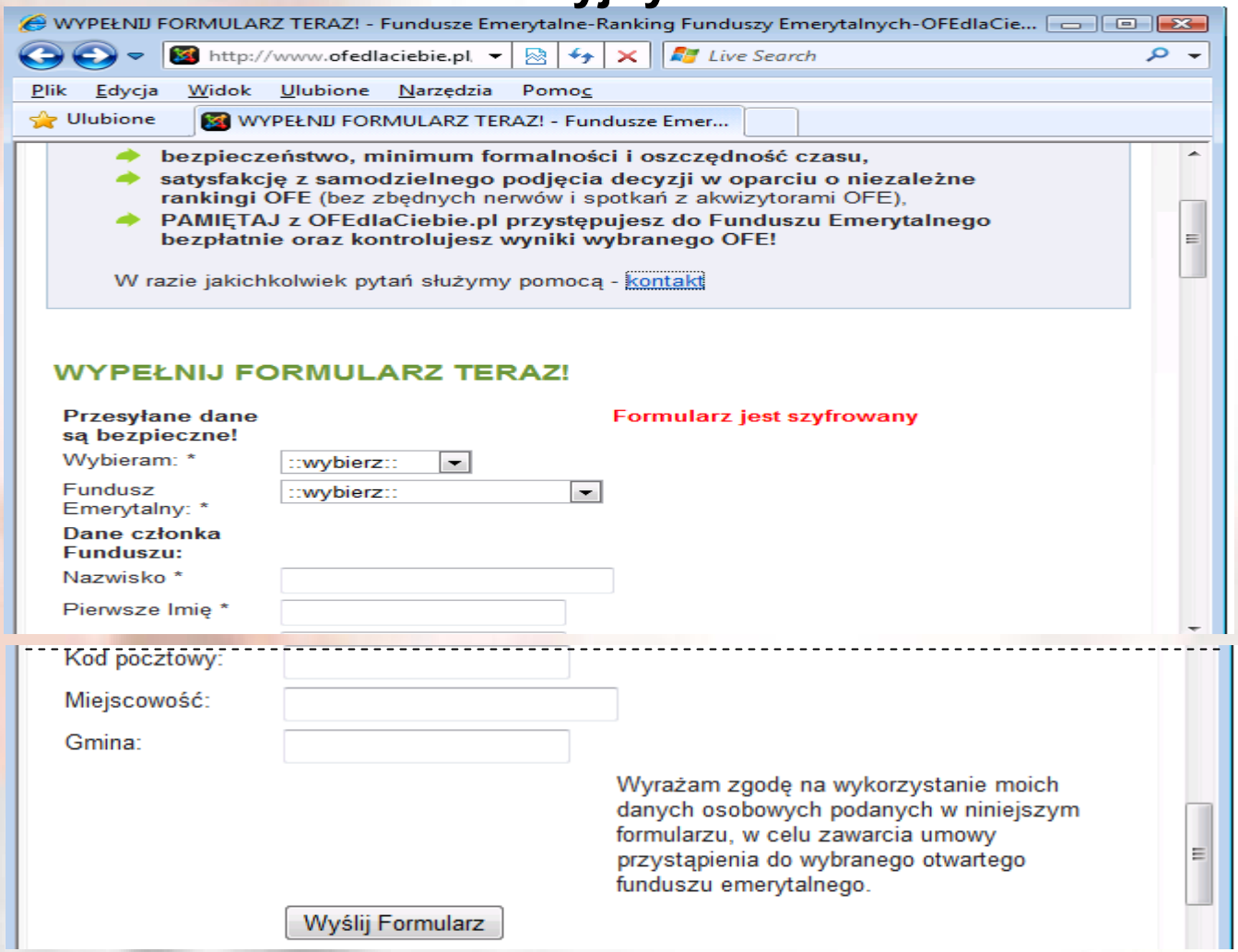
PRZYKŁADY (3)

Nieprawidłowe informacje o celu przetwarzania



ZŁE PRAKTYKI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

PRZYKŁADY (4) Nieprawidłowo wykonany obowiązek informacyjny



GIODO
Generalny Inspektor Ochrony Danych Osobowych

Dziękuję za uwagę!

Andrzej Kaczmarek

email: A_Kaczmarek@giodo.gov.pl

www.giodo.gov.pl