

KONIECZNE ZMIANY W PRZEPISACH ROZPORZĄDZENIA Z PUNKTU WIDZENIA GIODO

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

PLAN

- ❑ Obecny kształt regulacji w zakresie funkcjonalności i bezpieczeństwa
- ❑ Obecny poziom wypełniania przez ADO warunków technicznych i organizacyjnych przetwarzania danych
- ❑ Obserwowane kierunki zmian w architekturze systemów informatycznych
 - wymagania w zakresie rozliczalności
 - wymagania w zakresie bezpieczeństwa
- ❑ Wymagania dotyczące raportowania zawartości rejestrów i wymiany danych między nimi
- ❑ Możliwe kierunki przyszłych regulacji

WYMAGANIA WYNIKAJĄCE Z ART. 32 USTAWY (Wymagania dotyczące funkcjoności)

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,**
- 5e. uzyskania informacji o **przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2.**

Art. 38

Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane

WYMAGANIA WYNIKAJĄCE Z § 7 UST. 1 ROZPORZĄDZENIA (Wymagania dotyczące funkcjoności)

§ 7 ust. 1 Rozporządzenia

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

- 1. daty pierwszego wprowadzenia danych do systemu;**
- 2. identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;**
- 3. źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;**
- 4. informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;**
- 5. sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy**

WYMAGANIA WYNIKAJĄCE Z ART. 36, 37 USTAWY (Wymagania dotyczące bezpieczeństwa)

Art. 36 ust. 1.

1. 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, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.
3. Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

Art. 37

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

WYMAGANIA WYNIKAJĄCE Z Załącznika do rozporządzenia (Wymagania dotyczące bezpieczeństwa)

I

- 1) Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, **zabezpiecza się przed dostępem osób nieuprawnionych** na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
- 2) Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest **dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej** do przetwarzania danych osobowych.

II

- 1) W systemie informatycznym służącym do przetwarzania danych osobowych **stosuje się mechanizmy kontroli dostępu** do tych danych.
- 2) Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
 - a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
 - b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i **dokonaniu uwierzytelnienia**.

WYMAGANIA WYNIKAJĄCE Z Załącznika do rozporządzenia (Wymagania dotyczące bezpieczeństwa)

IV

- 1) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
- 2) W przypadku gdy do uwierzytelniania użytkowników używa się hasła, **jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.**
- 3) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
- 4) Kopie zapasowe:
 - a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;;
 - b) usuwa się niezwłocznie po ustaniu ich użyteczności.

WYMAGANIA WYNIKAJĄCE Z Załącznika do rozporządzenia (Wymagania dotyczące bezpieczeństwa)

VIII

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne

IX

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych

XII

- 1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem**
- 2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:**
 - a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;**
 - b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.**

ZAPISY ROZPORZĄDZENIE

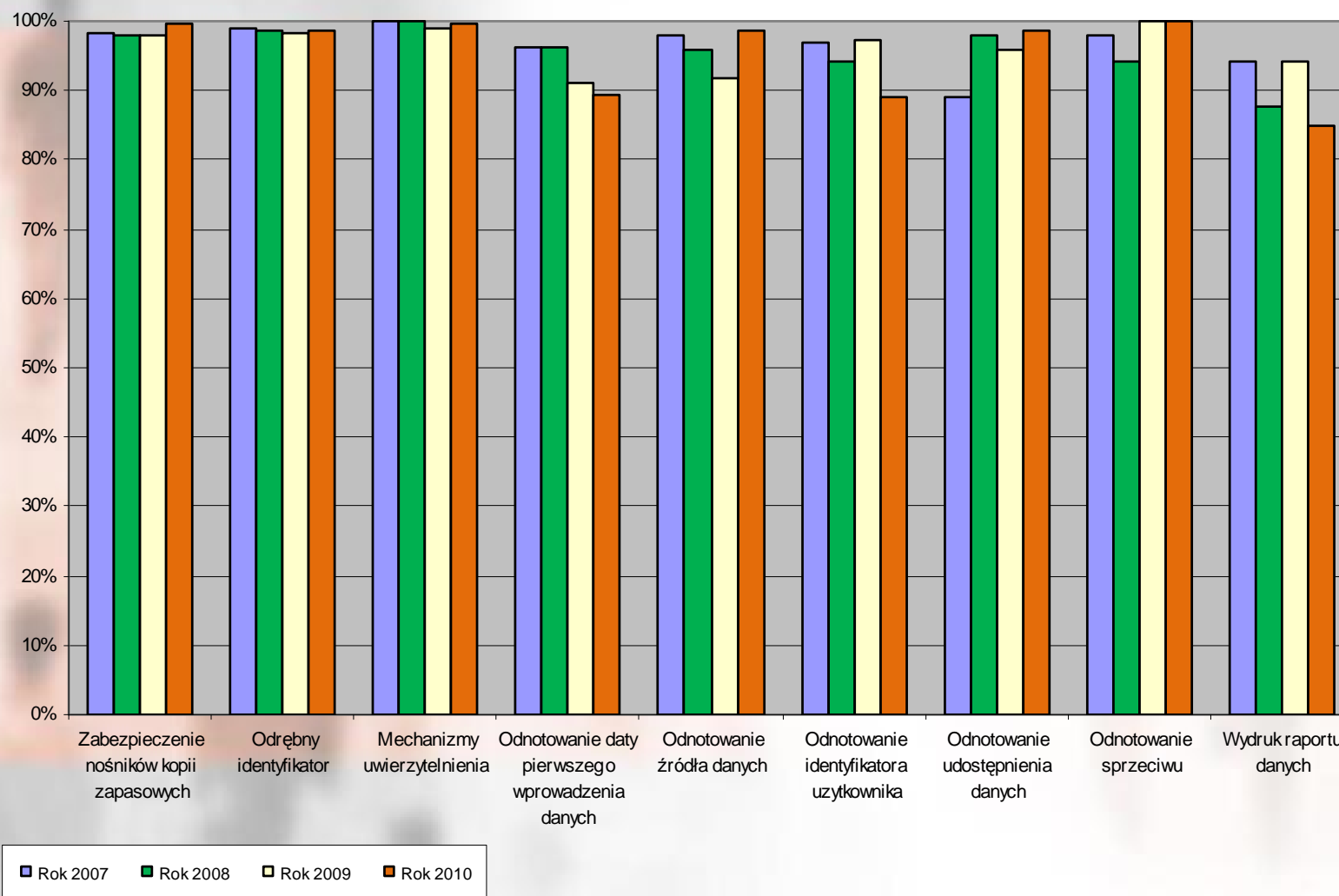
Wymagające modyfikacji

Zapisy rozporządzenia budzące najwięcej wątpliwości? (wymagające modyfikacji)

- 1) Obszar przetwarzania danych osobowych (jak wskazywać obszar w przypadku komputerów mobilnych, np. spis powszechnościowy);**
- 2) Brak rozróżnienie użytkownika systemu, którym jest osoba będąca pracownikiem administratora danych przetwarzająca dane klientów od użytkownika, który uzyskał uprawnienia tylko do wprowadzania/ modyfikacji swoich własnych danych.**
- 3) Złożoność i częstotliwość zmiany hasła – czy i jak należy zróżnicować wymagania dotyczące uwierzytelnienia, aby były one klarowne i kompletne.**
- 4) Brak przepisu wskazującego wprost obowiązek ochrony kryptograficznej danych przesyłanych wprost przy użyciu sieci bezpiecznej np. protokołu https.**

NAJCZĘŚCIEJ WYSTĘPUJĄCE UCHYBIENIA

Realizacja wymogów o charakterze techniczno-organizacyjnym w latach 2007-2010



OBECNA ROLA ROZPORZĄDZENIA

- 1. Rola regulacyjna (wskazanie wymagań funkcjonalnych i bezpieczeństwa)**
- 2. Rola edukacyjna (wskazano wprost minimalne wymagania dla powszechnie stosowanych rozwiązań)**

Wady rozwiązania

- 1. Nie uwzględnia wszystkich możliwych scenariuszy zagrożeń**
- 2. Szybko się dezaktualizuje**
- 3. Zamyka możliwość stosowania rozwiązań alternatywnych wobec wymienionych w rozporządzeniu**

Zalety rozwiązania

- 1. Podpowiada wprost jakościowy i ilościowy sposób wypełniania niektórych wymagań**
- 2. Wskazuje kluczowe, minimalne wymagania**
- 3. Jest powszechnie i nieodpłatnie dostępne**

JAKI KIERUNEK WYBRAC

1. Rozwiązania dedykowane i bardziej szczegółowe (rozporządzenia)
2. Rozwiązania również szczegółowe ale centralne (rozporządzenie, standardy, normy)

Przykład rozwiązań centralnych

1. Rozwiązanie Niemieckie - BSI
2. Rozporządzenie dotyczące bezpieczeństwa systemów (odnoszące się do wszystkich podmiotów)
3. Odwołanie do norm i standardów Europejskich, Międzynarodowych, Innych

Przykład rozwiązań dedykowanych

1. Rozporządzenie dotyczące bezpieczeństwa danych osobowych
2. Rozporządzenie dotyczące bezpieczeństwa informacji niejawnych
3. Rozporządzenie dotyczące bezpieczeństwa systemów medycznych

UNIWERSALNY CHARAKTER SRODKÓW BEZPIECZEŃSTWA INFORMATYCZNEGO

- Środki ochrony danych przetwarzanych w systemach informatycznych nie są zależne od rodzaju danych (osobowe, finansowe, handlowe, technologiczne – know how)
- Zagrożenia bezpieczeństwa rosną wraz z wartością danych
- Środki ochrony danych zależne są od środowiska, w którym są przetwarzane (rodzaj systemu operacyjnego, bazy danych, protokołów transmisji)

-
- Standardy międzynarodowe np. ISO/IEC 27000
 - Standardy Europejskie np. EN 12251 - Secure User Identification for Health Care - Management and Security of Authentication by Passwords
 - Dobre praktyki np. ITIL, ISACA(COBIT)
 - Standardy dostawców technologii np. MBSL, branżowe

Opinia 3/2010 dotycząca zasad odpowiedzialności

Przyjęta w dniu 13lipca 2010 r

Celem opinii jest wsparcie ochrony danych w praktyce poprzez zaproponowanie Komisji zmian jakie należy wprowadzić do dyrektywy. Zmiany te powinny spowodować przejście od teorii ochrony danych do praktyki. Opinia uwzględnia tezy zawarte w dokumencie WP 168 Grupy Art. 29 z grudnia 2009 r. zatytułowanego „The Future of Privacy”

- Sugeruje się, że mechanizmy odpowiedzialności za ochronę danych stanowiąc będą w przyszłości dla administratorów danych główne narzędzie zwiększania efektywności ich ochrony.
- Podkreśla się, że w celu zapewnienia odpowiedzialności za dane administratorzy powinni zastosować odpowiednie i efektywne środki, które skutecznie pozwolą wypełniać postanowienia dyrektywy. Środki te na żądanie powinny być zademonstrowane.
- Uzupełnieniem mechanizmów odpowiedzialności powinny być specjalne wymagania odnoszące się do bezpieczeństwa skutkujące zwiększeniem skuteczności zastosowanych środków. Wskazuje się na potrzebę wprowadzenie wymogu szacowania wpływu operacji przetwarzania danych na ochronę prywatności w przypadku podwyższonego ryzyka.

Opinia 3/2010 dotycząca zasad odpowiedzialności – cel i narzędzia

- Celem zwiększenia odpowiedzialności za ochronę danych jest poprawa efektywności stosowanych zabezpieczeń. Potrzeba ta wynika z wzrostu ilości i wartości przetwarzanych danych. Wzrost ten jest szczególnie dynamiczny w środowisku sieci informatycznych (portale społecznościowe, handel elektroniczny, usługi administracji publicznej, usługi służby zdrowia, bankowe, komunalne, w tym inteligentne opomiarowanie).
- Jednym z narzędzi nakłaniających administratorów do stosowania środków ochrony mogą być zasady odpowiedzialności dodane w wyniku rewizji dyrektywy. Zasady te powinny zobowiązać do stosowania wewnętrznych środków i procedur zapewniających skuteczną ochronę. Procedury te mogą się różnić w zależności od istniejącego ryzyka i rodzaju danych.
- Ponadto, należy rozważyć zastosowanie szczególnych wymagań takich jak obowiązek przeprowadzenia wpływu zastosowanego rozwiązania na ochronę prywatności lub obowiązek wyznaczenia inspektora bezpieczeństwa (data protection officers).

Opinia 3/2010 dotycząca zasad odpowiedzialności – konkretne propozycje

Nowe regulacje powinny wspierać stosowanie praktycznych narzędzi wprowadzając w ten sposób ustanowione zasady do konkretnych polityk ochrony i procedur. Powinny one koncentrować się na:

- **obowiązku wprowadzenia przez administratora skutecznych środków ochrony**
- **konieczności wykazania na żądanie organu, że skuteczne środki zostały zastosowane**

W opinii podkreśla się, że rodzaje środków ochrony nie muszą być wyspecyfikowane w ogólnych zasadach odpowiedzialności.

Minimalne ilościowe i/lub jakościowe wymagania dotyczące takich środków dla określonych przypadków mogą być specyfikowane przez:

- **Krajowe Biura Ochrony Danych Osobowych,**
- **Grupę roboczą Art.. 29, lub**
- **Komisję Europejską.**

Dziękuję za uwagę

Andrzej Kaczmarek

BIURO

GENERALNEGO INSPEKTORA OCHRONY
DANYCH OSOBOWYCH