PRZETWARZANIE DANYCH OSOBOWYCH

proInfoSec
Jarosław Żabówka
proinfosec@odoradca.pl

13 czerwiec 2011

Wymogi rozporządzenia

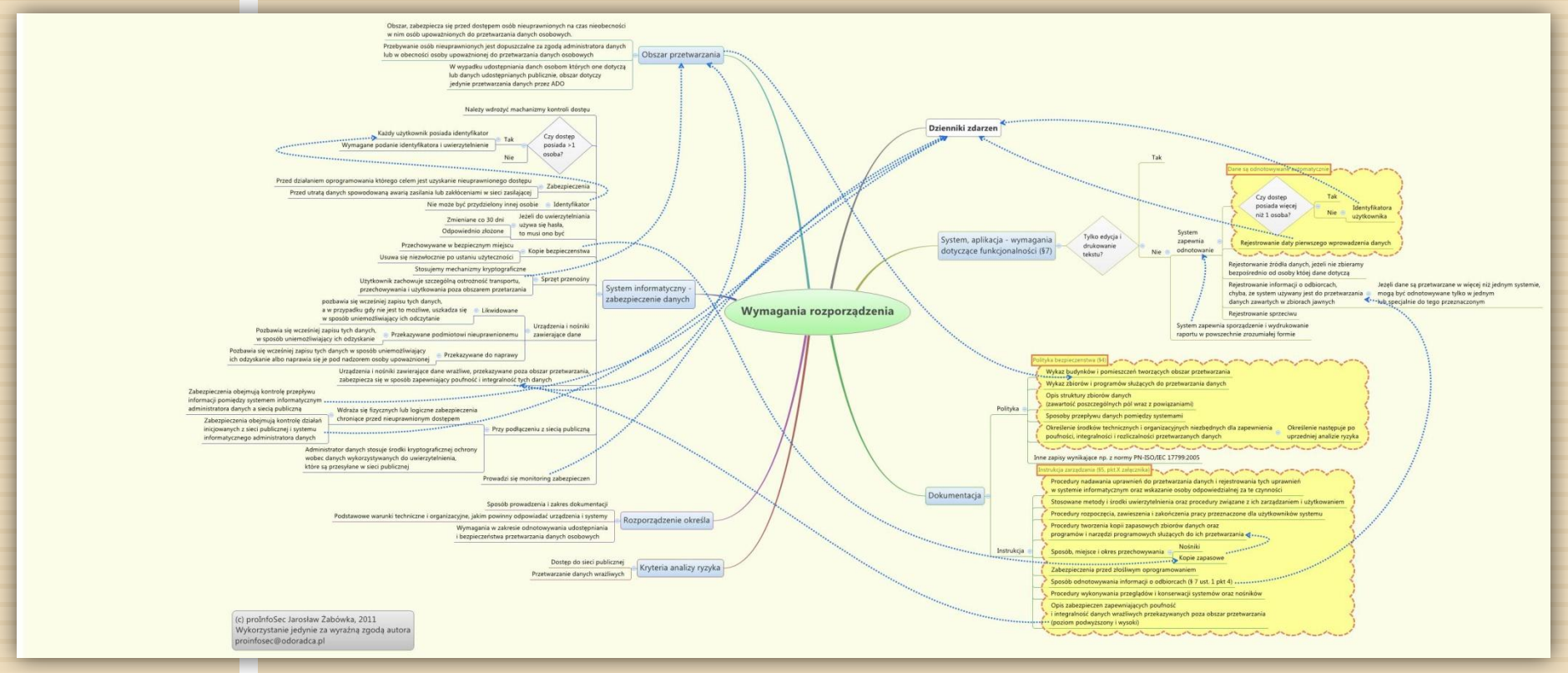
ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

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

Zawartość prezentacji

- W czasie trwania prezentacji omówimy wybrane zagadnienia regulowane rozporządzeniem.
- Omawiając zabezpieczenia, ograniczymy się do zabezpieczeń wymaganych na poziomie wysokim.



4

Zawartość prezentacji

W kilku miejscach prezentacji korzystać będziemy z maindmap-y przedstawiającej regulowane rozporządzeniem zagadnienia

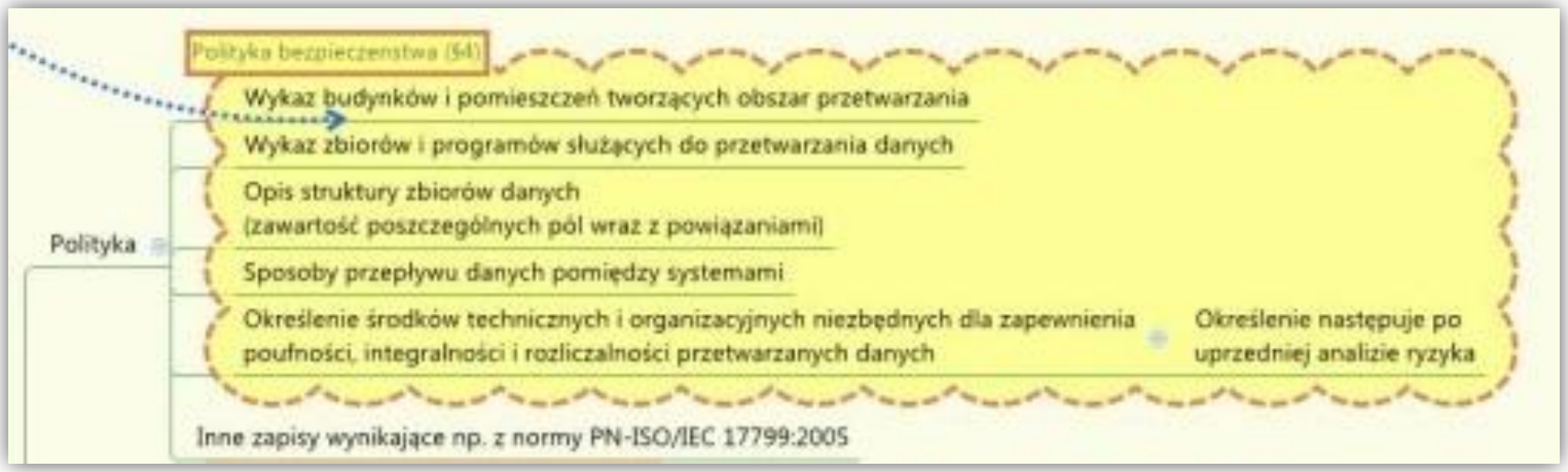
Podstawa rozporządzenia

- **Art. 39a.** Minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

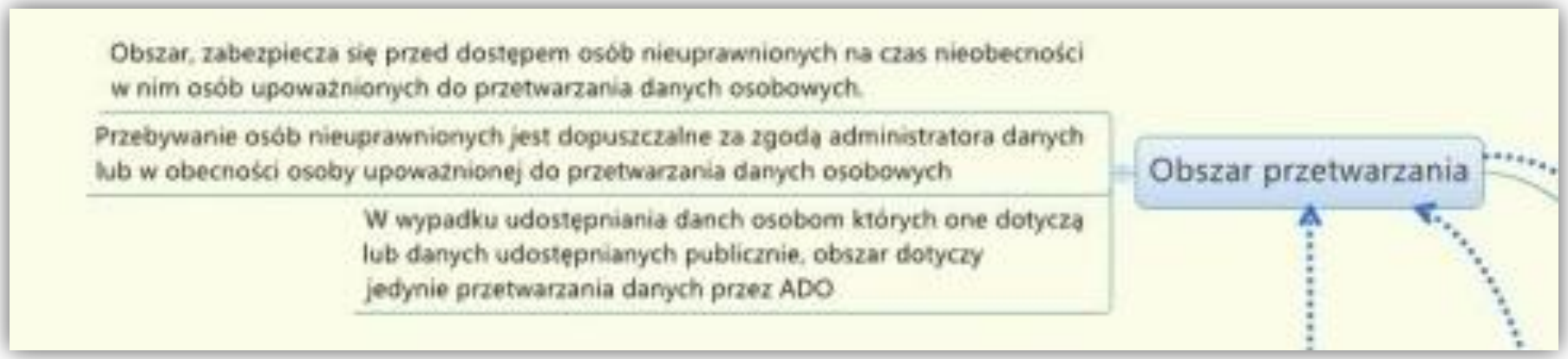
Zakres regulacji rozporządzenia

- Sposób prowadzenia i zakres dokumentacji
- Podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy
- Wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych

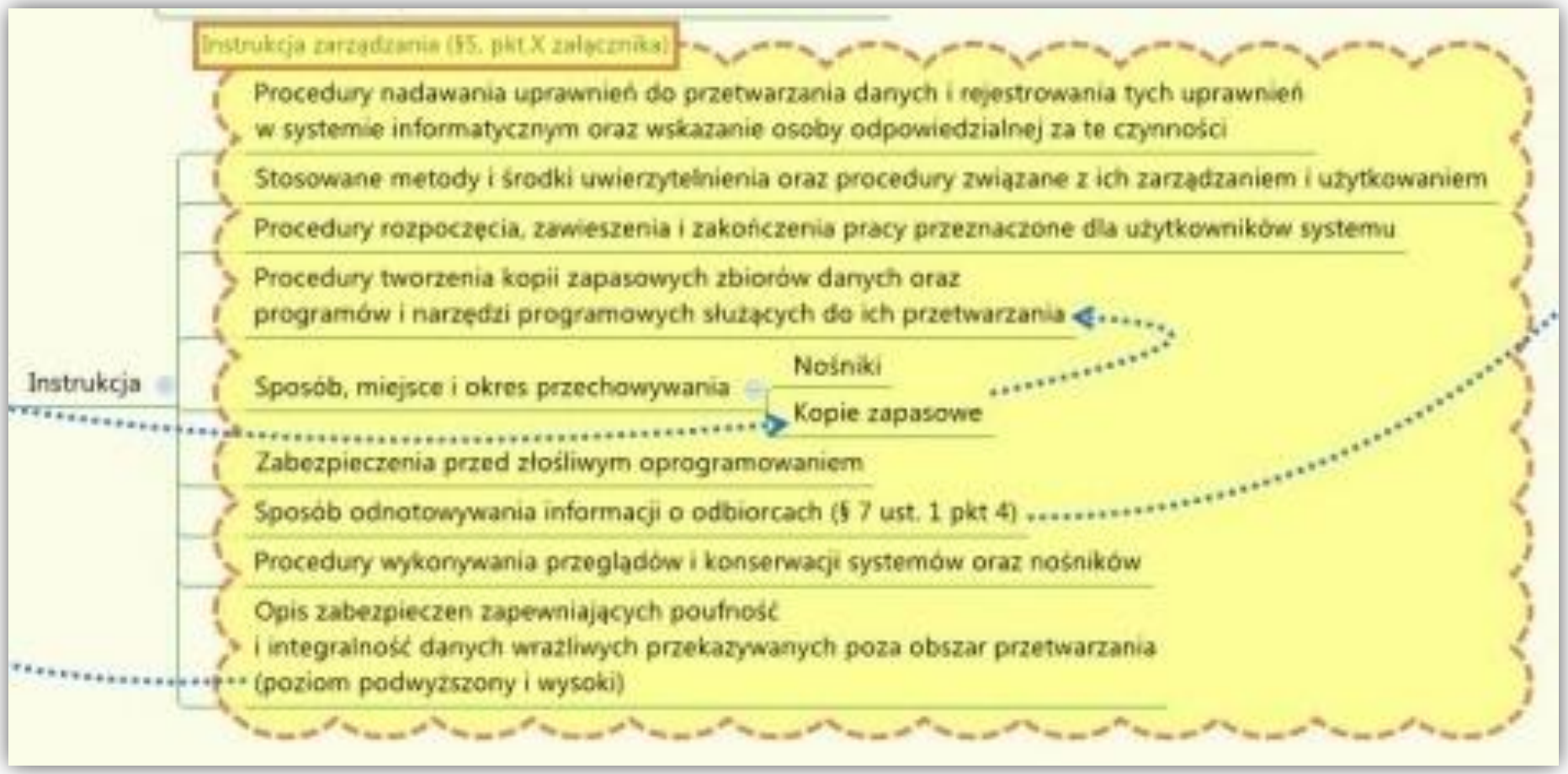
Polityka bezpieczeństwa



Obszary przetwarzania



Instrukcja zarządzania



Wymagania dotyczące funkcjonalności

- **Art. 32. 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 w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej,
  - **5)** uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
  - **5a)** 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 dotyczące funkcjonalności

§ 7.

1. 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.

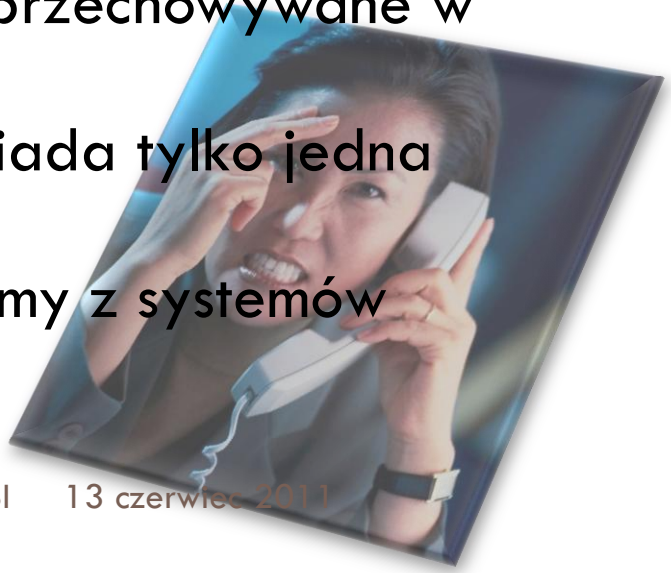
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

Wymagania dotyczące funkcjonalności

Jak się bronić?

- Żądajmy wymaganych funkcjonalności od dostawcy oprogramowania - ale przecież nawet Urzędy Skarbowe miały wpadkę i korzystały z oprogramowania nie spełniającego wymogów!
- Zauważmy, że automatycznie odnotowane muszą być spełnione jedynie wymagania określone w 2 pierwszych punktach.
- Informacje o udostępnieniu mogą być przechowywane w osobnym systemie.
- Zapewnijmy, że dostęp do danych posiada tylko jedna osoba...
- Jeżeli mamy taką możliwość, korzystajmy z systemów jedynie dla sporządzania wydruków...



Co robić gdy arkusz kalkulacyjny jest dla nas wystarczający?

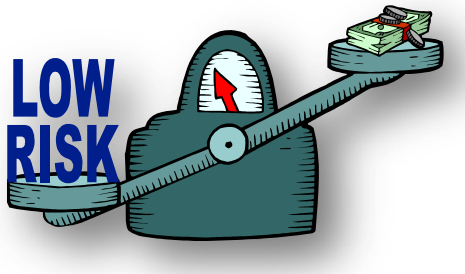
Zabezpieczenie danych

Art. 36. 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

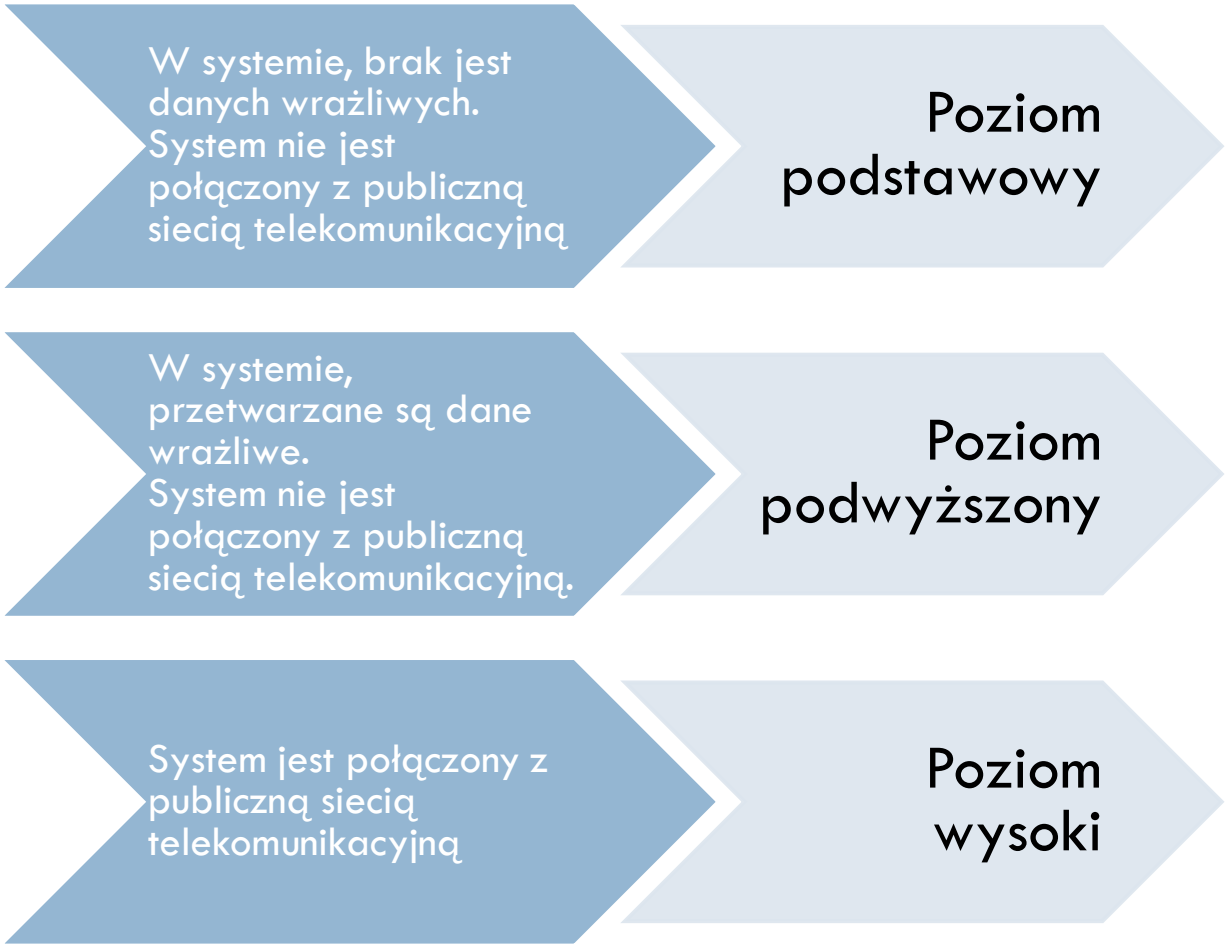
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

Rozporządzenie jako analiza ryzyka

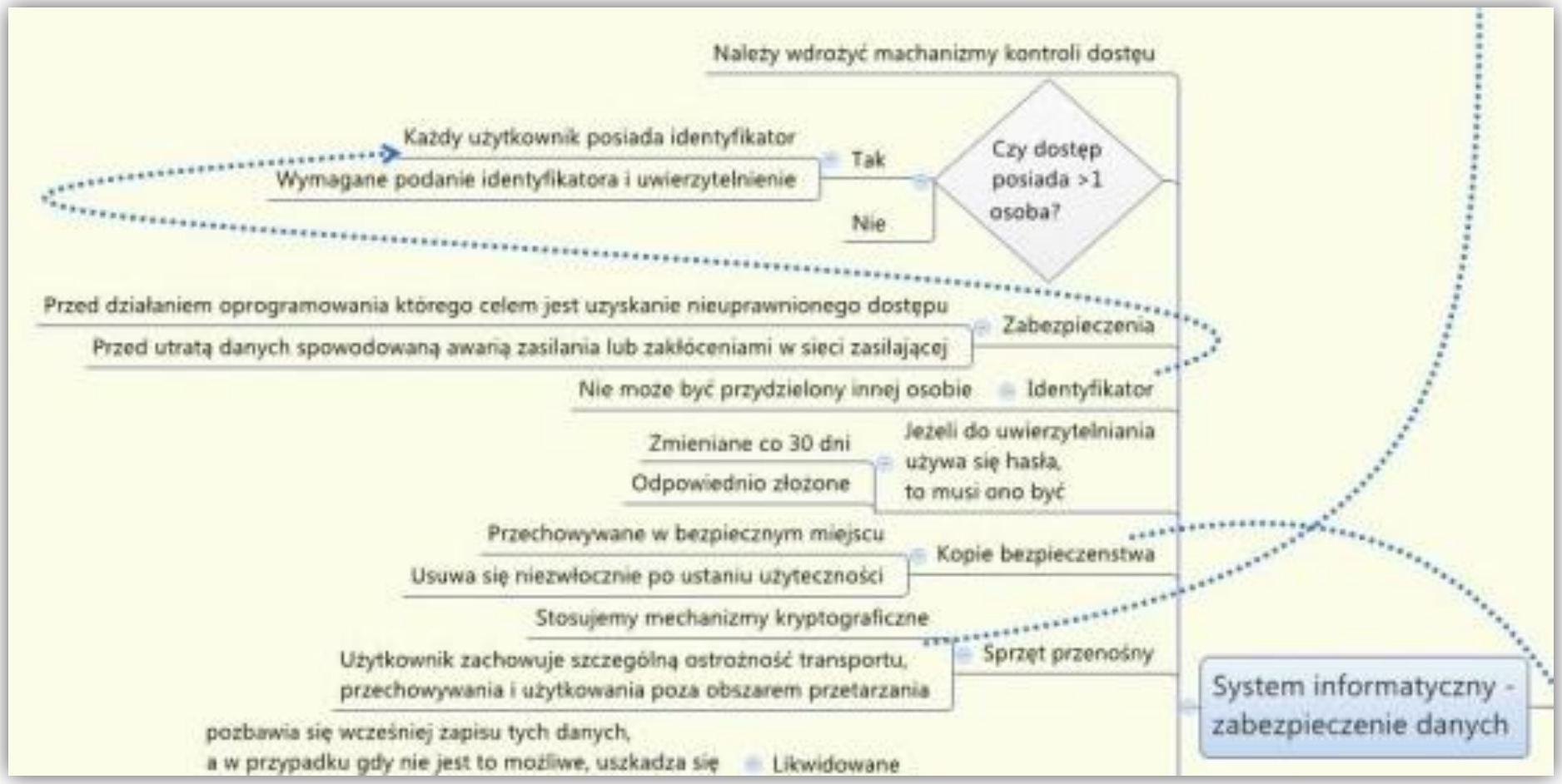
- Rozporządzenie wskazuje jakie zabezpieczenia należy stosować. Można uznać, że w rozporządzeniu została przyjęta bardzo uproszczona analiza ryzyka, opierająca się jedynie na kryteriach:
  - dostępu do sieci publicznej
  - przetwarzaniu danych wrażliwych.



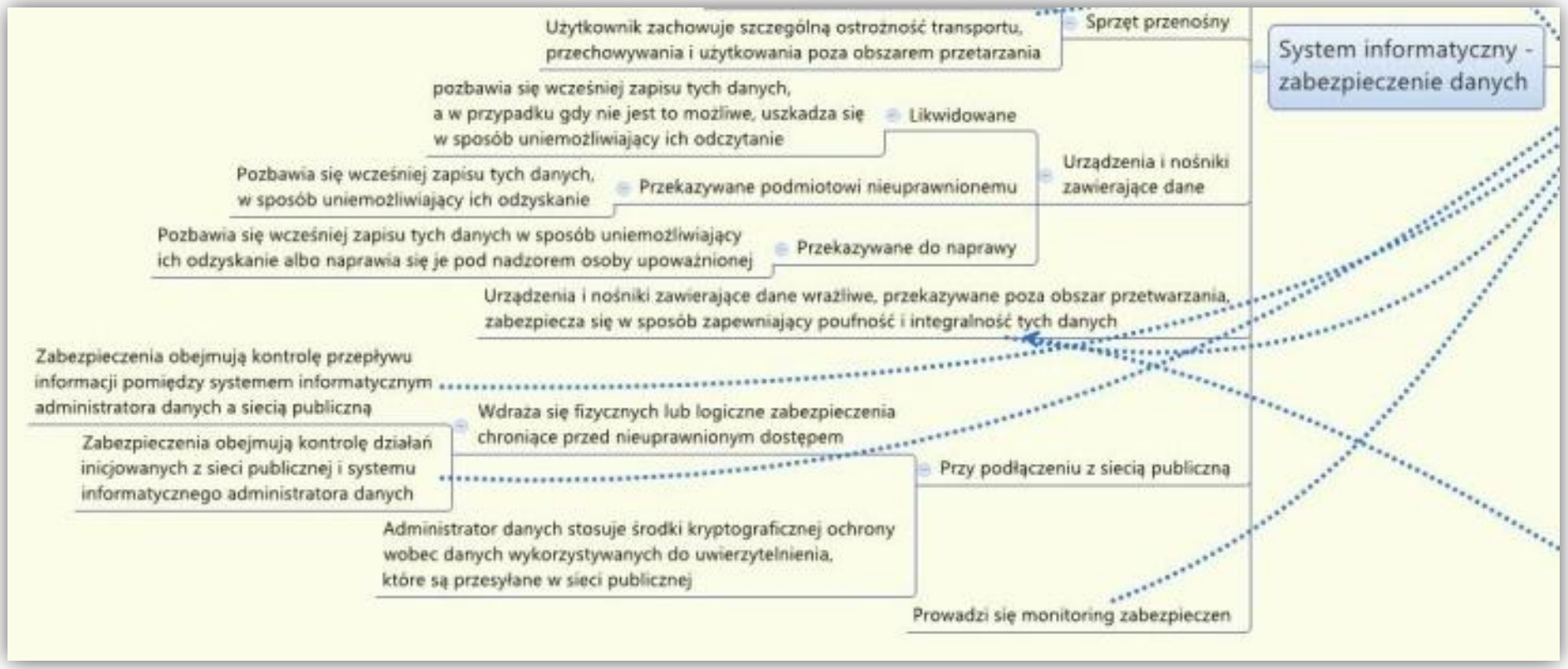
Poziomy bezpieczeństwa



Zabezpieczenia



Zabezpieczenia



Problemy

- Nieżyciowe wymagania w stosunku do aplikacji.
- Obszary przetwarzania – nie uwzględniają sprzętu mobilnego, pracy zdalnej i pracy w terenie (spis powszechny!)
- Brak rozróżnienia użytkownika, od osoby która uzyskuje dostęp jedynie do swoich danych.
- Brak przepisu nakazującego stosowanie środków kryptograficznych przy przesyłaniu danych przez sieć publiczną.

Konieczna nowelizacja. Ale jaka?

- Nowe rozporządzenia?
- Danie GIODO prawa publikowania obowiązujących rekomendacji?
- Oparcie się o normy i/lub analizę ryzyka?
- A może jakieś inne rozwiązanie?

BARDZO DZIĘKUJEMY ZA UWAGĘ I ZAPRASZAMY DO DYSKUSJI.