Normalizacyjna mapa RODO – co mamy dziś i jakie są perspektywy

Dr inż. Elżbieta Andrukiewicz

Przewodnicząca KT182 Ochrony Informacji w Systemach Teleinformatycznych przy Polskim Komitecie Normalizacyjnym

Ekspert ISO, Edytor norm międzynarodowych

„Nowe zasady zabezpieczenia danych osobowych, czyli RODO w praktyce”
GIODO, 28.03.2018r

Plan prezentacji

- Wprowadzenie ontologiczne konieczne do zrozumienia norm
- Historia lat ostatnich normalizacji wspierającej RODO… pasmo europejskich niepowodzeń i światełko w tunelu
- Mapa norm referencyjnych w odniesieniu do wymagań RODO
- Krótka prezentacja jądra normalizacji – certyfikacja w RODO
- Plany KT 182 - wsparcie dla wdrożenia RODO – co możemy zrobić dziś
- Plan pracy dla norm międzynarodowych w obszarze prywatności

Ontologiczne podejście do prywatności

- Pojęcia i terminy należy umieścić w kontekście, aby zweryfikować ich odpowiedniość, równoważność albo sprzeczność
  - Kontekst normalizacyjny jest inny niż prawny czy regulacyjny

- W normach technologicznych ISO/IEC JTC 1/SC27 „prywatność” jest pojęciem (konceptem) nie definiowanym
  - prywatność jest charakteryzowana przez szereg atrybutów
    - prywatność cielesna, prywatność miejsca pobytu i otoczenia, prywatność zachowania, prywatność komunikowania się, prywatność danych i wizerunku, prywatność myśli i uczuć oraz prywatność relacji (wyliczenie z PrPN-ISO/IEC 29134)
  - oraz towarzyszących terminów (zob. PN ISO/IEC 29100)
    - naruszenie prywatności – sytuacja, w której informacje identyfikujące osobę są przetwarzane z pogwałceniem jednego lub więcej wymagań zabezpieczenia prywatności
    - ryzyko prywatności – efekt niepewności w odniesieniu do prywatności

Prywatność -> PII -> dane osobowe

- Kontekst prywatności w normach technologicznych ogranicza się do systemów teleinformatycznych
  - Terminem podstawowym jest ‚informacja identyfikująca osobę' - personally identifiable information (PII)
- Charakterystyka PII jest szersza niż charakterystyka danych osobowych, jednakże:
- RODO dotyczy też przetwarzania poza systemami teleinformatycznymi

PII - dowolna informacja, która:

(a) może być użyta do zidentyfikowania osoby, do której się odnoszą lub

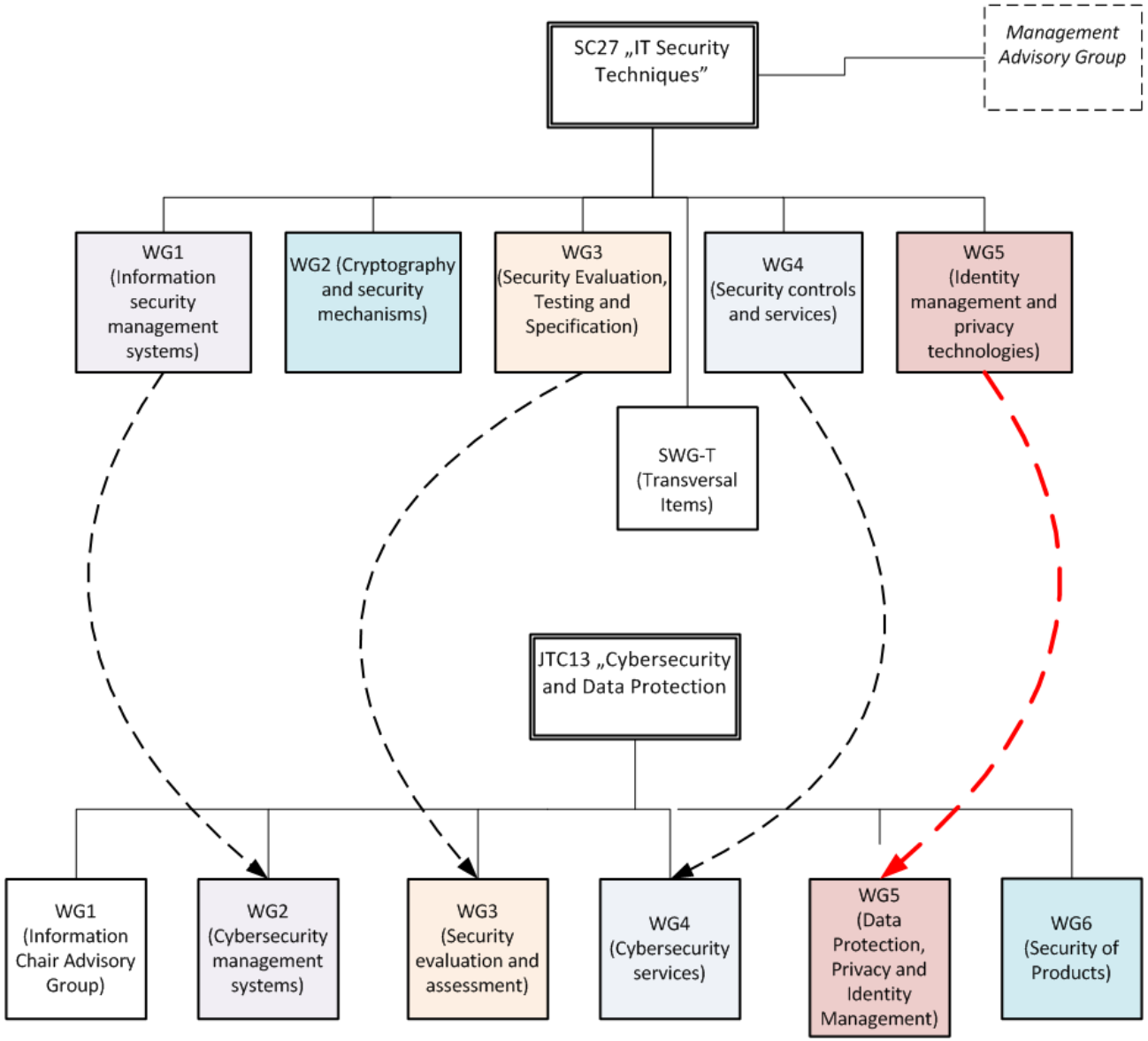
(b) mogłaby być bezpośrednio lub pośrednio powiązana z osobą, do której się odnosi

„dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (RODO)

Ciernista droga norm europejskich do RODO

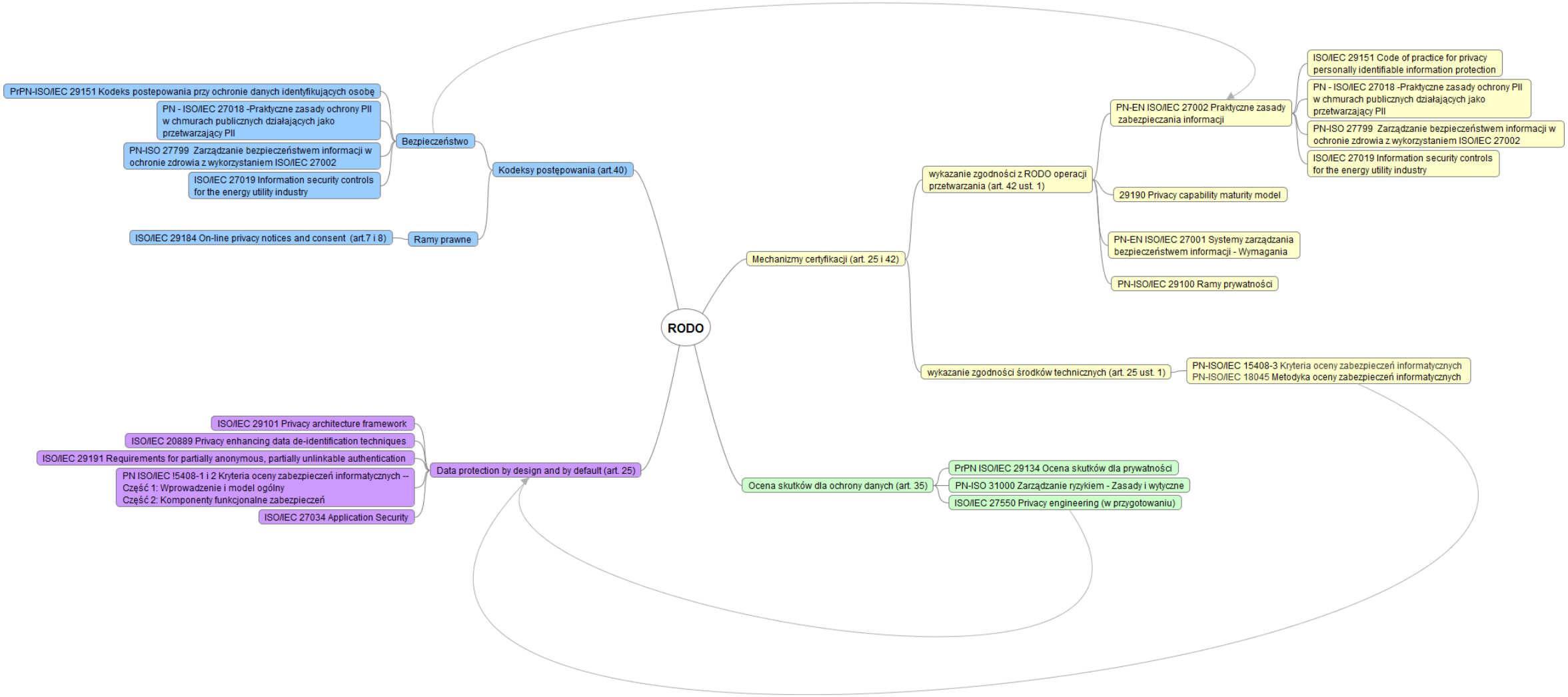
- 2014: CEN/CENELEC JWG 8 „Privacy management in products and services”
  - scope the development of norms and standards in support of GDPR implementation
  - Mandat Komisji Europejskiej
  - Liczba opracowanych/ adaptowanych norm: 0
- 2017: utworzenie CEN/CENELEC JTC 13 „Cybersecurity and Data Protection”
  - 11’ 2017: 1. posiedzenie JTC13
  - 02’2018: wyodrębnienie grup roboczych
  - 06’ 2018: postanowione rozwiązanie JWG8 i przejęcie tematyki przez JTC 13
- CEN/CENELEC przypomniały sobie o istnieniu porozumień z Wiednia (ISO-CEN) oraz Frankfurtu (CENELEC – IEC), określających zasady współpracy przy tworzeniu norm

Linia transmisyjna norm ISO do Europy



- W planie działania JTC13 zakłada się przyjmowanie norm międzynarodowych jako norm europejskich
- KT 182 jest „lustrzanym” komitetem, zarówno dla SC27, jak i dla JTC13

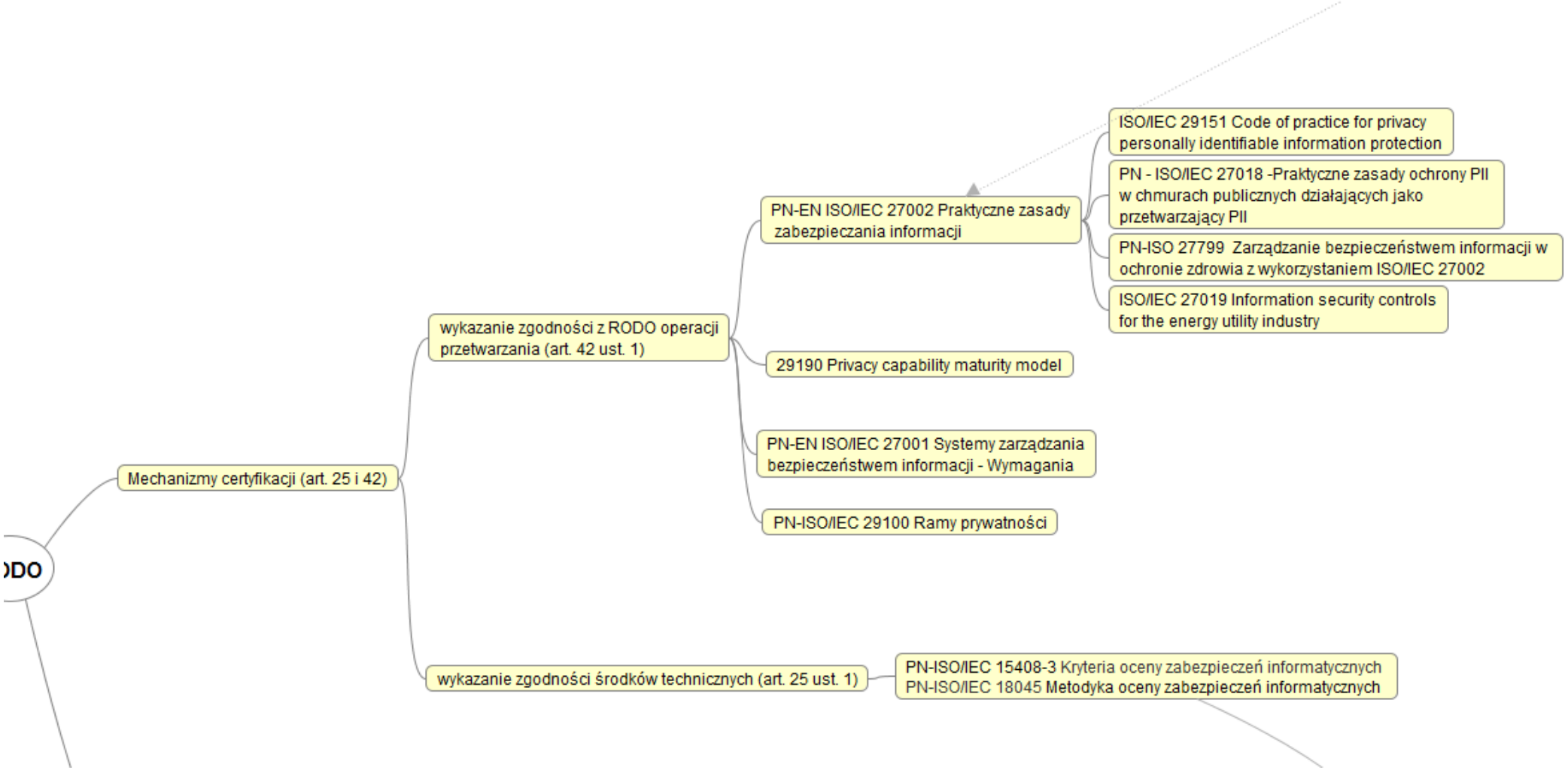
Mapa norm referencyjnych dla RODO (JTC1/SC27)



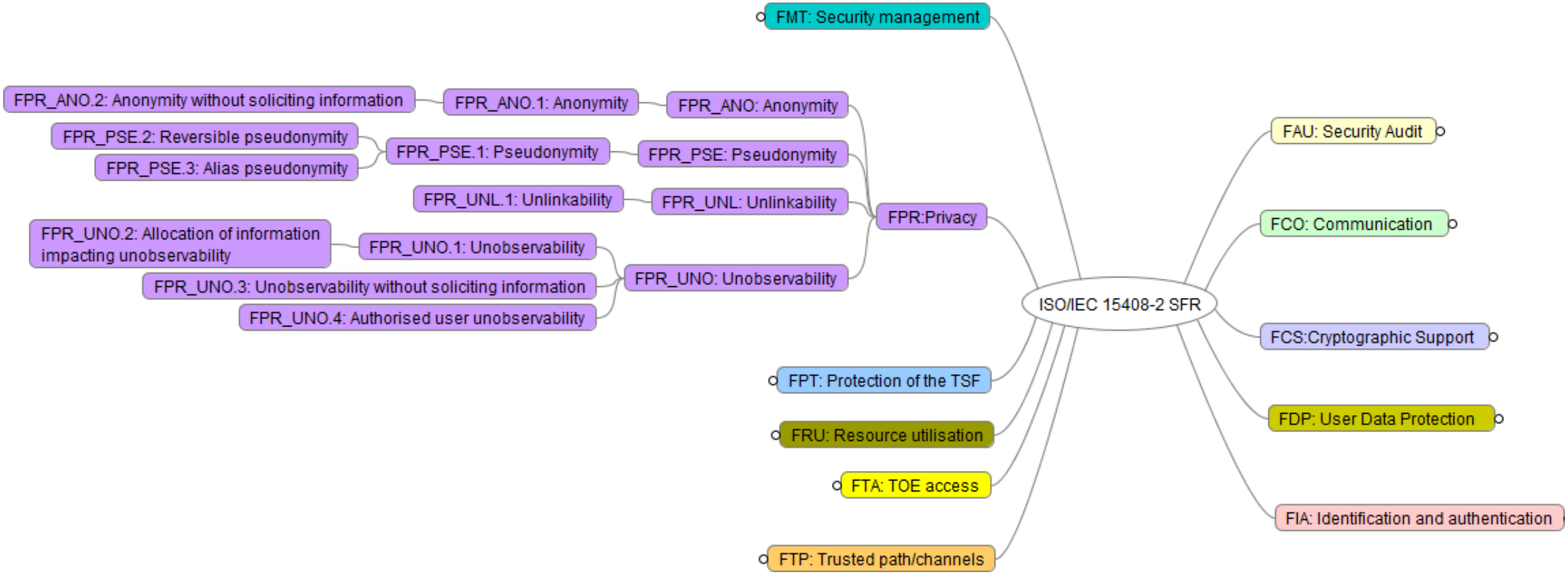
Rodzaje mechanizmów certyfikacji w RODO – są DWA

- Certyfikacja przedmiotowa – Art. 25 ust. 1 oraz 3
  - (..) *Administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie* ***środki techniczne*** *i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.*
  - *Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.*
- Certyfikacja procesowa (podmiotowa) - Art. 42 ust. 1
  - Wdrażanie „*mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem* ***operacji przetwarzania*** *prowadzonych przez administratorów i podmioty przetwarzające”.*

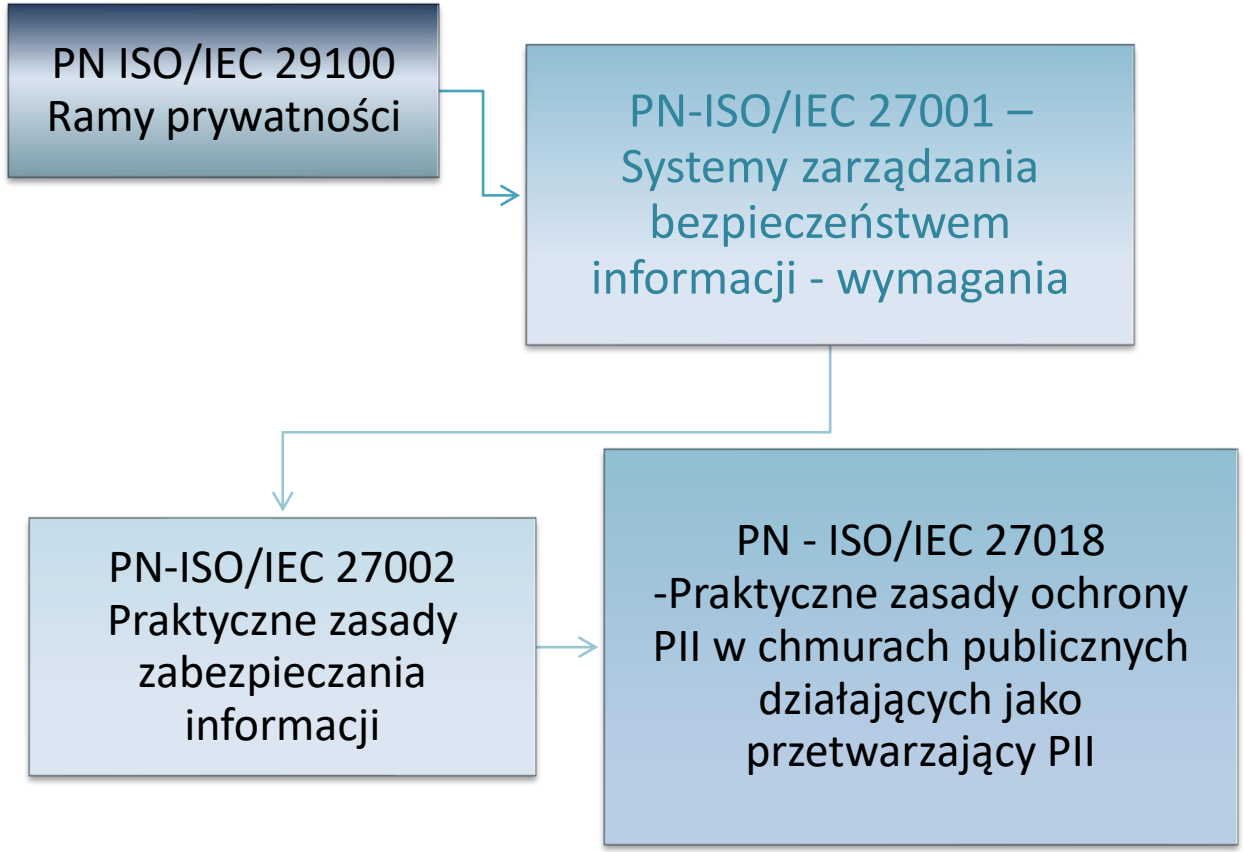
Normy referencyjne dla mechanizmów certyfikacji



Wymagania w klasie prywatności wg. normy PN-ISO/IEC 15408-2



Normy referencyjne dla certyfikacji systemów zarządzania w obszarze prywatności



=> ISO/IEC 27552 „Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management – Requirements and guidelines

Aktualne działania KT 182

Norma	Tytuł	Aktualny stan w systemie PN
EN ISO/IEC 27001:2017	Information Security Management Systems - Requirements / Systemy Zarządzania Bezpieczeństwem Informacji - Wymagania	Tłumaczanie PN-EN ISO/IEC 27001:2017-06
EN ISO/IEC 27002:2017	Code of practice for information security controls / Praktyczne zasady zabezpieczania informacji	Tłumaczanie PN-EN ISO/IEC 27002:2017-06
EN ISO/IEC 27000:2017	Information Security Management Systems - Overview and Vocabulary / Systemy Zarządzania Bezpieczeństwem Informacji - Przegląd i terminologia	Tłumaczenie* PrPN EN ISO/IEC 27000
ISO/IEC 29100:2011	Privacy framework/ Ramy prywatności	Uznanie PN ISO/IEC 29100:2017-07
ISO/IEC 29101: 2013	Privacy architecture framework/ Ramy architektury prywatności	Uznanie PN-ISO/IEC 29101: 2017-07
ISO/IEC 27017:2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Uznanie PN ISO/IEC 27017:2017-07
ISO/IEC 27018:2014	Code of practice for PII protection in public clouds acting as PII processors / Praktyczne zasady ochrony PII w chmurach publicznych działających jako przetwarzający PII	Uznanie PN-ISO/IEC 27018:2017-07
ISO/IEC 15408-x :2009 (x=1,2,3)	Evaluation Criteria for IT security/ Kryteria oceny zabezpieczeń informatycznych	Uznanie PN-ISO/IEC 15408-x:2016-10
ISO/IEC TR 18045:2008	Methodology for IT security evaluation/ Metodyka oceny zabezpieczeń informatycznych	Uznanie PN-ISO/IEC TR 18045:2016-10
ISO/IEC 29134:2017	Guidelines for privacy impact assessment/ Wytyczne dotyczące oceny skutków dla prywatności	Tłumaczenie PrPN-ISO/IEC 29134
ISO/IEC 29151:2017	Code of practice for personally identifiable information protection/ Kodeks postępowania przy ochronie danych identyfikujących osobę	Tłumaczenie PrPN-ISO/IEC 29151
*norma europejska przyjeta metodą uznaniową 2017-06		

Plan pracy SC27/WG5

Nr normy	Tytuł	Oczekiwana data publikacji
ISO/IEC 27550	Privacy engineering	sie-19
ISO/IEC 20889	Privacy enhancing data de-identification techniques	wrz-19
ISO/IEC 27552	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management – Requirements and Guidelines	lis-19
ISO/IEC 29184	Guidelines for online privacy notices and consent	mar-20
ISO/IEC 27551	Requirements for attribute-based unlinkable entity authentication	lis-20
NWIP*	Privacy Guidelines for Smart Cities	?
SP**	Potential internationalisation of DIN 66398 Guideline for development of a concept for data deletion with deviation of deletion periods for personal identifiable information	?
SP	Framework of user-centric PII handling based on privacy preference management by users	?
SP	Application of ISO 31000 for identity-related risk	?

* New Work Item Proposal

**Study Period

Pytania?