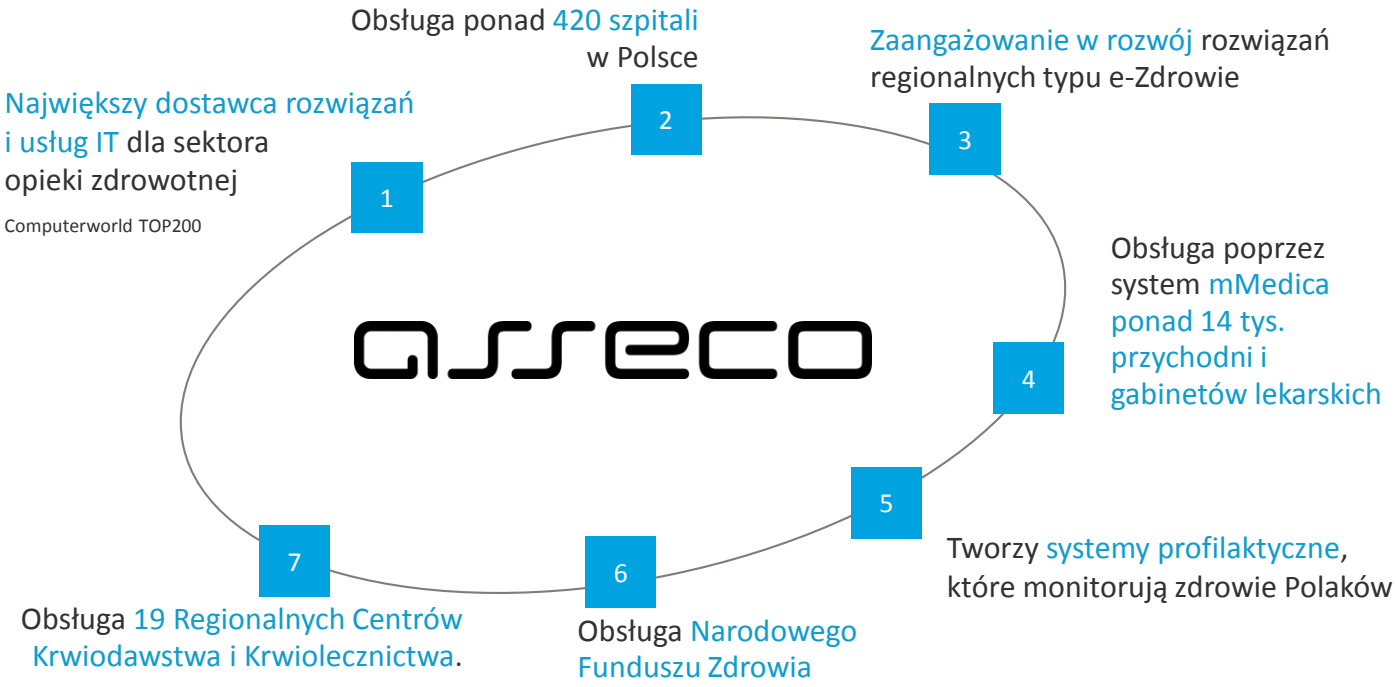
Prywatność i bezpieczeństwo danych medycznych

Realizacja w praktyce nowych wymagań wynikających z wprowadzenia RODO

Janusz Jasłowski

Gdańsk, 14 września 2017 r.

Pozycja Asseco na polskim rynku medycznym



Nowe wyzwania wynikające ze zmian legislacyjnych

1. Ustawa wprowadzająca tzw. sieć szpitali
2. Wytyczne i rekomendacje dotyczące EDM
3. **R**ozporządzenie o **O**chronie **D**anych **O**sobowych /The **G**eneral **D**ata **P**rotection **R**egulation /RODO = GDPR/

RODO

27 kwietnia 2016

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych
- RODO /Rozporządzenie o Ochronie Danych Osobowych/ = GDPR /The General Data Protection Regulation/
- obowiązek stosowania wejdzie w życie 25.05.2018 r.

Główne cele:

- **zapewnienie skutecznej ochrony danych osobowych** w zmieniających się warunkach: technologicznych, gospodarczych, organizacyjnych
- **zapewnienie jednolitego prawa w całej Europie**

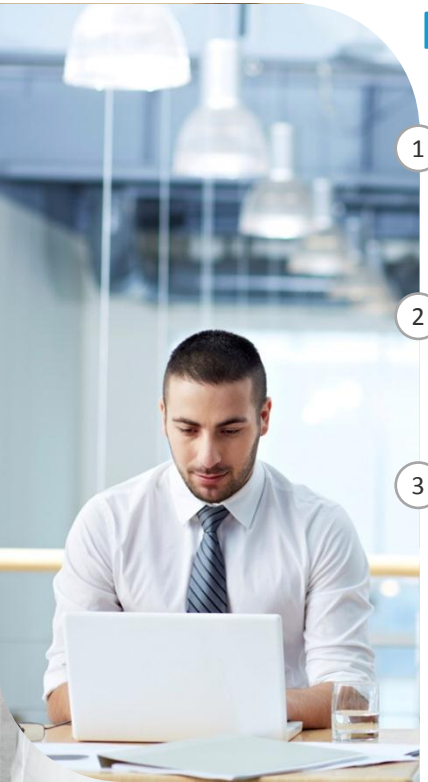
Wpływ RODO na jednostki medyczne

Powołanie Inspektora Danych Osobowych

1. Inspektor, względem ABI, posiadać będzie dodatkowe obowiązki:
   - → monitorowanie i egzekwowanie przestrzegania zasad ochrony danych,
   - → zgłaszanie naruszeń ochrony danych osobowych,
   - → prowadzenie rejestru naruszeń bezpieczeństwa danych, rejestru czynności i przetwarzania,
   - → odpowiadanie na zapytania / skargi osób, których dane dotyczą.
2. Za naruszenie przepisów grozi kara pieniężna do 100.000 zł

(art. 49-50 projektu ustawy z 28.03.2017r. o ochronie danych osobowych).

Wpływ RODO na jednostki medyczne



Powierzenie przetwarzania DM podmiotom zewnętrznym

1. Można korzystać tylko z usług podmiotów, które zapewniają wystarczające gwarancje (art. 28 ust 1).
2. Potwierdzeniem wiarygodność takich gwarancji może być uzyskanie certyfikatu.
3. Za naruszenie przepisów grozi kara pieniężna do 10.000.000 EUR lub do 2% całkowitego rocznego światowego obrotu przedsiębiorcy.

Wpływ RODO na jednostki medyczne

Ocena ryzyka przetwarzania danych

1. Jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności osób z racji swego charakteru, zakresu lub celów:
   - → GDPR rozszerzył katalog danych wrażliwych, a także doprecyzował jakie dane należy rozumieć pod pojęciem „danych dotyczących zdrowia”
   - → Prawdopodobnie regulacje krajowe wymuszą na podmiotach leczniczych obowiązek sporządzania takiej ocena ryzyka
2. Za naruszenie przepisów grozi kara pieniężna do 10.000.000 EUR lub do 2% całkowitego rocznego światowego obrotu przedsiębiorcy.

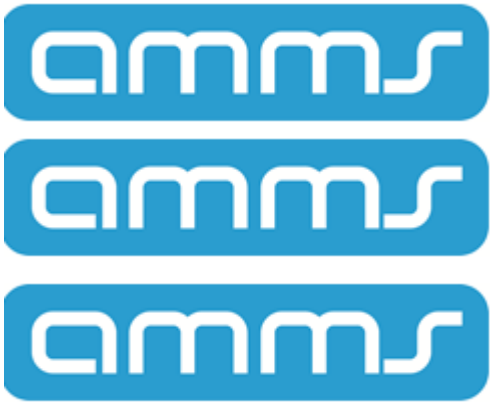
Jak realizować przepisy GDPR

Zasadne jest kierowanie się zalecanymi kodeksami postępowania oraz poddawaniu się Certyfikacji

Certyfikat będzie obowiązywał 3 lata.

GDPR wskazuje te mechanizmy (kodeksy, certyfikacje) jako wskazane dla uzasadniania zgodności z prawem jak również dla wyznaczania wymagań wobec potencjalnych oferentów w ramach postępowań przetargowych.

Realizacja wytycznych GDPR, a system informatyczny



Dostosowanie systemów informatycznych w szczególności w zakresie:

1. wspomagania pracy inspektora,
2. realizacji szczegółowych wytycznych dot. zgód, prawa do zapomnienia,
3. wspomaganie oceny ryzyka.

Korzyści wprowadzenia nowych rozwiązań

dla jednostki medycznej i pacjenta

1. Możliwość wyboru podmiotów przetwarzających dane, które zapewniają gwarancje określone prawem.

2. Ułatwienie wywiązywania się ze swoich obowiązków w zakresie ochrony danych, w tym uzasadniania zgodności z prawem przed Prezesem Urzędu Ochrony Danych Osobowych.

Korzyści wprowadzenia nowych rozwiązań

dla jednostki medycznej i pacjenta

③ Kluczowy aspekt dla wizerunku
– zaufanie pacjentów co do bezpieczeństwa ich danych i transparentności ich przetwarzania.

④ Możliwość szybkiej oceny poziomu bezpieczeństwa danych osobowych przetwarzanych w danym podmiocie.

Podsumowanie

Przed jednostkami medycznymi wiele nowych obowiązków i odpowiedzialności, jako administratorów danych osobowych:

1. umiejętność wykazania przetwarzania danych w zgodności z prawem,
2. konieczność powołania inspektorów ochrony danych,
3. część regulacji dotyczy systemów informatycznych.

Z poziomu dostawcy rozwiązań IT prowadzimy przygotowania do pełnego wdrożenia przepisów GDPR i EDM.

Janusz.Jaslowski@asseco.pl

asseco.pl

Solutions for demanding business.

Zastrzeżenia prawne

Zawartość dostępna w prezentacji jest chroniona prawem autorskim i stanowi przedmiot własności. Teksty, grafika, fotografie, dźwięk, animacje i filmy, a także sposób ich rozmieszczenia w prezentacji podlegają ochronie na mocy Ustawy o prawach autorskich i prawach pokrewnych oraz innych przepisów z tym związanych. Jakiekolwiek nieautoryzowane zastosowanie jakichkolwiek materiałów zawartych w prezentacji może stanowić naruszenie praw autorskich, znaków firmowych lub innych przepisów. Materiały dostępne w prezentacji nie mogą być modyfikowane, powielane, przedstawiane publicznie, wykonywane, rozprowadzane lub wykorzystywane w innych celach publicznych lub komercyjnych, chyba że Asseco Poland S.A. wydał na to wyraźną zgodę na piśmie. Kopiowanie w celach komercyjnych, rozpowszechnianie, modyfikacja lub przejmowanie zawartości niniejszej prezentacji przez osoby trzecie jest niedozwolone. W prezentacji mogą być prezentowane również materiały zawierające odesłania do ofert i usług podmiotów trzecich. Warunki korzystania z ofert i usług podmiotów trzecich są określone przez te podmioty. Asseco Poland S.A. nie ponosi żadnej odpowiedzialności za warunki i skutki korzystania z ofert i usług tychże podmiotów. Dane i informacje zawarte w prezentacji mają jedynie charakter ogólnoinformacyjny. Prezentacja przygotowana została w oparciu i przy użyciu produktów firmy Inscale.

Nazwa oraz logo Asseco Poland S.A. są zarejestrowanymi znakami towarowymi. Korzystanie z tych znaków wymaga wyraźnej zgody ze strony Asseco Poland S.A.