IT i RODO z perspektywy zarządzającego podmiotem leczniczym

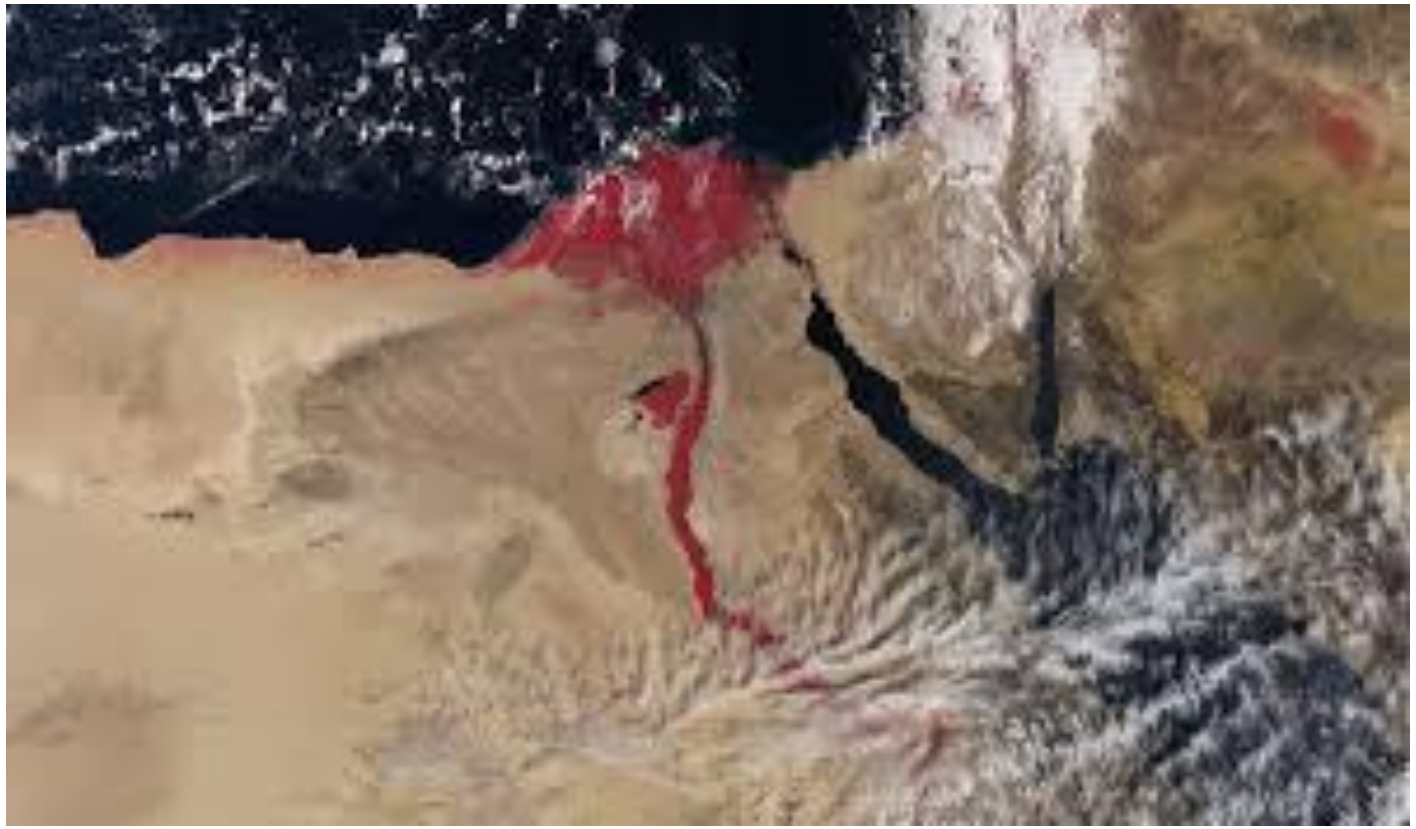
Beata Jagielska
Centrum Onkologii – Instytut im. Marii Skłodowskiej – Curii w Warszawie

Gdzie inspektor danych osobowych nie pomoże …tam prawnika pośle…….

W nawiązaniu do pisma……, w związku z różnymi interpretacjami przedstawionych problemów proszę zwrócić się z pytaniami do prawników……

Jedenasta plaga egipska RODO…….

- Szkolenie
- Wdrażanie
- Monitorowanie



Ochrona zdrowia i życia ….a….teraz RODO

- Tajemnica lekarska a…RODO
- Ochrona życia i zdrowia …a RODO

RODO a …IT

- Bezpieczeństwo danych w IT
- Bezpieczeństwo elektronicznej dokumentacji medycznej
- Bezpieczeństwo poczty elektronicznej
- Bezpieczeństwo danych administracyjnych

Kto jest administratorem danych?

Niebo europejskie

Nie kopiuj infrastruktury 1:1

Informacja o „obcym” niebie

Niebo światowe

Czy chmura zawsze jest bezpiecznym środowiskiem dla przetwarzanych danych osobowych?

Podmioty oferujące usługę cloud computing korzystają często z infrastruktury zewnętrznej, również współdzielonej przez kilku usługodawców. Równie często podmioty te, z uwagi na złożoność procesów zachodzących w chmurze, posiłkują się szeregiem podwykonawców, odpowiedzialnych za poszczególne elementy kompleksowej usługi cloud computing. Powoduje to, że operacje na danych umieszczonych w chmurze podejmują liczne, często anonimowe dla administratora podmioty. Sytuacja taka, z punktu widzenia przepisów ustawy o ochronie danych osobowych, jest niedopuszczalna.

umowa z dostawcą usługi wyraźnie określa, jakie podmioty i w jakim zakresie uzyskują dostęp do przetwarzanych w chmurze danych osobowych

Konieczności zawarcia pisemnej umowy o powierzenie przetwarzania danych osobowych.

Podmiot przetwarzający dane na zlecenie administratora spełnia wymogi określone w tzw. programie Safe Harbor.(poza EOG)

Umowa o powierzeniu przetwarzania danych winna określać fizyczną lokalizację serwerów

https://www.computerworld.pl/news/Chmura-na-swiecie-i-w-Polsce-piec-powodow-wolniejszej-implementacji,407257.html

RODO a badania kliniczne

- Przetwarzanie danych osobowych osób uczestniczących w badaniu klinicznym następuje zawsze na podstawie **zgody osoby uprawnionej** (art. 6 ust. 1 lit. a RODO)
- Informacja dla uczestnika badania w sprawie przetwarzania jego danych osobowych na potrzeby badania
- Czy komisja bioetyczna może oceniać zgodność informacji z RODO?

RODO a badania kliniczne

- **Obowiązek informacyjny wobec osób, których dane osobowe są zbierane bezpośrednio od nich (art. 13 RODO) - informacje:**
  - Dane administratora, jego przedstawiciela oraz inspektora ochrony danych
  - Cele przetwarzania oraz podstawa prawna
  - o odbiorcach danych/ ich kategoriach
  - Okres przechowywania danych
  - o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu

RODO a badania kliniczne

- o prawie żądania dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych
- o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem
- o prawie wniesienia skargi do organu nadzorczego
- czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są **ewentualne konsekwencje niepodania danych**

RODO a badania kliniczne

- O innym celu przetwarzania - jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane
- o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia

RODO a badania kliniczne

❑Problemy praktyczne:

- **Przekazywanie danych do państw poza EOG:**

✓tylko ogólna informacja, że poziom ochrony jest niższy niż w UE

✓podejmą działania w celu zapewnienia ochrony zgodnej z prawem (jakim? RODO, czy prawem państwa trzeciego?)

✓ogólne zapewnienie o zapewnieniu wysokiego poziomu ochrony

✓**Powinno być zapewnienie, że ochrona danych osobowych będzie zgodna z RODO**

RODO a badania kliniczne

- ✓Najlepiej, gdy są ustalone wiążące reguły korporacyjne (Binding Corporate Rules), albo przekazanie następuje wyłącznie do państwa, co do którego KE stwierdziła spełniania wymagań
- ✓Czy zgoda badanego jest wystarczająca? - musi być poinformowana i wyraźna oraz udzielona dobrowolnie, czyli nie będzie właściwą podstawą, gdyby zachodziła sytuacja nie równorzędności podmiotów
- Brak swobodnego kontaktu w zakresie ochrony danych – kontakt w innym państwie nieobsługiwany w języku polskim

Notatka wizualna od Agaty Jakuszko z rozmowy z Tomaszem Palakiem – Ustawa RODO strona WWW.