DZP

więcej niż prawo

RODO i cyberbezpieczeństwo w placówkach medycznych

- stan obecny i perspektywy na przyszłość

Agata Kruczyk-Gonciarz,

Associate DZP, 780 115 035

agata.kruczyk-gonciarz@dzp.pl

Poznań, październik 2018 r.

Agenda prezentacji

Węzłowe problemy podmiotów wykonujących działalność leczniczą w związku z RODO

Kodeks branżowy dla ochrony zdrowia

Cyberbezpieczeństwo

DZP

Węzłowe problemy podmiotów wykonujących działalność leczniczą w związku z RODO

6 miesięcy po rozpoczęciu obowiązywania RODO

Żądania pacjentów dotyczące danych osobowych – liczne skargi pacjentów	Zawieranie umów powierzenia przetwarzania – kiedy jest to niezbędne?	Zapewnienie anonimowości pacjentów w procesie udzielania świadczeń
Sposób wypełniania obowiązków wynikających z RODO	Konieczność zbierania zgód na przetwarzanie danych osobowych	Brak praktyki i jednoznacznego stanowisk PUODO w niektórych kwestiach

DZP

Kodeks branżowy – stan prac

- Merytoryczna część prac nad kodeksem branżowym w ochronie zdrowia jest już prawie zamknięta (trwają jeszcze prace nad uregulowaniem zasad monitorowania kodeksu)
- Konsultacje projektu przebiegały bardzo aktywnie – zgłoszono sporo uwag.
- W przyszłym tygodniu planujemy wszcząć procedurę zatwierdzania kodeksu przez PUODO.
- Do postępowania w przedmiocie zatwierdzania projektu kodeksu zastosowanie mają znaleźć przepisy kodeksu postępowania administracyjnego – co do zasady więc kodeks powinien zostać zatwierdzony w terminie 2 miesięcy od dnia jego złożenia.
- Najnowszy projekt kodeksu znajduje się na stronie www.rodowzdrowiu.pl

DZP

Projekty wspierające podmioty wykonujące działalność leczniczą dotyczące RODO

Przewodnik po RODO w służbie zdrowia Ministerstwa Zdrowia i Ministerstwa Cyfryzacji - opublikowany

Kampania edukacyjna kierowana do pacjentów dotycząca RODO – kick-off w najbliższych tygodniach

DZP

Krajowy system cyberbezpieczeństwa – konsekwencja dla podmiotów leczniczych

• 1 sierpnia 2018 r. Prezydent RP podpisał ustawę ustanawiającą ramy prawne funkcjonowania krajowego systemu cyberbezpieczeństwa, który obejmować będzie m.in. podmioty lecznicze o strategicznym znaczeniu dla zapewnienia dostępności opieki zdrowotnej dla obywateli.

• Decyzję o włączeniu podmiotu leczniczego do krajowego systemu cyberbezpieczeństwa wydawać będzie Minister Zdrowia do dnia **9 listopada 2018** r. Decyzja ta podlegać będzie natychmiastowemu wykonaniu.

• Sankcje za nieprzestrzeganie nowych obowiązków – kary finansowe do 200 tys. złotych

• W związku z procedowanymi obecnie przepisami wykonawczymi należy się spodziewać, że do krajowego systemu cyberbezpieczeństwa zostaną włączone podmioty lecznicze, które:

- są zakwalifikowane do systemu podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej (tzw. sieci szpitali);
- posiadają dostęp do Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego;
- prowadzą dział farmacji szpitalnej i/lub aptekę szpitalną.

DZP

Nowe obowiązki dla podmiotów leczniczych zakwalifikowanych do systemu

3 miesiące od zakwalifikowania - wdrożenia **systemu zarządzania bezpieczeństwem**, w ramach którego zostaną opisane m.in. sposób zarządzanie zdarzeniami, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo oraz stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację (system zarządzania incydentami)

3 miesiące od zakwalifikowania - zapewnienie pacjentom **dostępu do wiedzy** pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa (w szczególności przez publikowanie informacji na swojej stronie internetowej) i stosowanie skutecznych sposobów zabezpieczenia przed tymi zagrożeniami.

6 miesięcy od zakwalifikowania - opracować, stosować i na bieżąco aktualizować **dokumentację dotyczącą cyberbezpieczeństwa**, w tym bezpieczeństwa systemów informacyjnych. Dodatkowo nad dokumentacją będzie zobowiązany ustanowić **nadzór**.

3 miesiące od zakwalifikowania - **wyznaczyć osobę** odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa

DZP

Działania do podjęcia na najbliższy czas

RODO

- Monitorowanie praktyki PUODO;
- Przeprowadzenie audytu powdrożeniowego;
- Organizacja szkoleń z personelem medycznym i administracyjnym – antidotum na „Absurdy RODO”.

Cyberbezpieczeństwo

- Przeprowadzenie szkolenia wewnętrznego dotyczącego zmian związanych z wdrożeniem krajowego systemu cyberbezpieczeństwa
- Przeprowadzenie audytu (we współpracy z ekspertami ds. IT) i przygotowanie odpowiednich procedur, wewnętrznych dokumentów oraz szkoleń pracowników

DZP

Biuro w Warszawie
Rondo ONZ 1
00-124 Warszawa
T + 48 22 557 76 00
F + 48 22 557 76 01

Biuro w Poznaniu
ul. Paderewskiego 8
61-770 Poznań
T + 48 61 642 49 00
F + 48 61 642 49 50

Biuro we Wrocławiu
ul. Gwiaździsta 66
53-413 Wrocław
T + 48 71 712 47 00
F + 48 71 712 47 50