Cyberdefence 24

aut. Sylwia Gliwa 15.11.2019

"CYBERNOWOTWÓR" POLSKIEJ SŁUŻBY ZDROWIA. POSYPIĄ SIĘ KARY OD PUODO?

Czy dane osobowe w podmiotach leczniczych są prawidłowo chronione i przetwarzane? Od czasu wejścia w życie RODO upłynęło już półtora roku a jednak jak wynika z najnowszego raportu Najwyżej Izby Kontroli zarówno w publicznych jak i niepublicznych jednostkach wciąż niezbyt pozytywnie wygląda poziom wprowadzenia unijnej regulacji. Wnioski nie napawają optymizmem i wskazują, że przed służbą zdrowia jeszcze bardzo długa droga, jeśli chodzi o wprowadzenie przepisów RODO w życie.

Generalne wnioski odnośnie wdrożenia przepisów RODO w kontrolowanych jednostkach wskazują, że polska służba zdrowia jest nieprzygotowana na funkcjonowanie zgodnie z narzuconymi przez unijną dyrektywę przepisami. Kontroli zostały poddane 24 podmioty lecznicze na terenie sześciu województw w kraju. Główny wniosek płynący z raportu pokazuje istotny problem: „Dane osobowe pacjentów nie były właściwie chronione i przetwarzane". Niemal w 67% podmiotów stwierdzono, że nie były one właściwie przygotowane do wejścia w życie RODO.

Gdzie szukać nieprawidłowości?

- W głównej mierze nie przestrzegano również zasad ograniczania dostępu do danych osobowych „do zakresu niezbędnego do osiągnięcia celu ich przetwarzania". Raport wykazał, że co 11 pielęgniarka miała dostęp do danych medycznych pacjentów leczonych na innych oddziałach szpitala.
- W 62,5% kontrolowanych jednostek nie odebrano niezwłocznie dostępu do systemów informatycznych byłym pracownikom.
- Dane osobowe pacjentów były również w sposób nieuprawniony przekazywane do podmiotów serwisujących systemy informatyczne – nieprawidłowość tą stwierdzono w 45,8% kontrolowanych jednostkach.
- Ignorowano także wymogi odnoszące się do nadawania właściwych uprawnień do administrowania systemami informatycznymi, ochrony przed złośliwym oprogramowaniem oraz odpowiedniej autoryzacji aż w 75% jednostkach. Natomiast aż w co piątej jednostce (20,8%) kopie bezpieczeństwa nie były przechowywane w niezabezpieczonych miejscach. Również w 75% podmiotów środki techniczne zastosowane do zabezpieczenia danych osobowych przechowywanych w postaci elektronicznej nie były wystarczające.

Problematycznym obszarem jest również wewnętrzna dokumentacja związana z bezpieczeństwem danych. W niemalże połowie kontrolowanych podmiotów (45,8%) nie dokonano aktualizacji podstawowej dokumentacji powiązanej z bezpieczeństwem danych osobowych oraz sposobów ich przetwarzania.

Odnotowano również drobny sukces – aż w 96% skontrolowanych jednostek wdrożono rozwiązania w których nie posługiwano się personaliami pacjentów. Zwrócono jednak uwagę, że rozwiązanie w których na wywieszanych listach pacjentów widniały tylko 3 pierwsze litery imienia i nazwiska nie chronią wystarczająco pacjentów o krótkich imionach i nazwiskach.

Ochrona antywirusowa? Nie jest aż tak źle. Gorzej z wykorzystaniem przestarzałego oprogramowania

W zaledwie 12,5% kontrolowanych jednostek na części komputerów nie zainstalowano oprogramowania antywirusowego a w 16,7% jednostek komputery nie posiadały aktualnych baz sygnatur wirusów. W dość nieszablonowy sposób jednostki lecznicze podchodzą do procesu autoryzacji użytkowników. W 50% jednostek, pracownicy w celu autoryzacji w systemach operacyjnych posługiwali się tymi samymi danymi. Dochodziło również do przypadków skrajnych – w 12,5% szpitali część komputerów nie wymagała uwierzytelniania w ogóle. Nikogo nie dziwi zatem fakt, że aż w 29,2% szpitalach stosowane hasła nie spełniały wewnętrznie ustalonych wymogów złożoności a w 50% jednostkach wykorzystywano systemy operacyjne, co do których producent zakończył wsparcie techniczne.

Posypią się kary od PUODO?

Aż 54,2% jednostki naruszyły zasady ochrony danych osobowych. Aż w 25% kontrolowanych jednostkach rodzaj naruszeń był na tyle istotny, że wymagał powiadomienia Prezesa Urzędu Ochrony Danych Osobowych.

Każda kontrolowana jednostka wyznaczyła inspektora ochrony danych. Jednak w niewielkiej części przeszkolono wszystkich pracowników z zakresu ochrony danych.

Wyniki kontroli Najwyższej Izby Kontroli wskazują na jeden generalny wniosek, że służba zdrowia cierpi na chroniczny brak ochrony danych swoich pacjentów i nie potrafi we właściwy sposób zaaplikować sobie leku chroniącego przed naruszeniami cyberbezpieczeństwa.