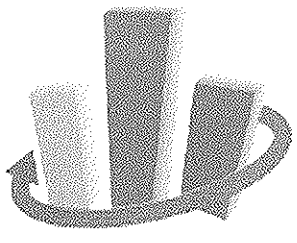

Polska Unia Szpitali Klinicznych

Nasz znak: 46/PUSK/2017

Poznań, 18 października 2017 r.

Szanowna Pani
Anna Streżyńska
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowna Pani Minister,

w odpowiedzi na prośbę o zgłaszanie ewentualnych uwag do:

1) projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych

2) projektu ustawy o ochronie danych osobowych

w załączeniu przekazuję uwagi zgłoszone przez członków Polskiej Unii Szpitali Klinicznych:

1. Samodzielny Publiczny Szpital Kliniczny Nr 2 PUM w Szczecinie,
2. Szpital Uniwersytecki w Krakowie.

Zgodnie z prośbą uwagi zostały również przekazane drogą elektroniczną.

W imieniu Zarządu

lek. med. Jan Talaga

Zał. 1

Stowarzyszenie *Polska Unia Szpitali Klinicznych*
REGON: 140544131
NIP: 5272520070

Adres do korespondencji
ul. Długa 1/2, 61-848 Poznań
e-mail: uniaszpitali@skpp.edu.pl

Uwagi dot. projekt ustawy o ochronie danych osobowych

1) Projekt ustawy o ochronie danych osobowych zakłada, że **jedynym** podmiotem uprawnionym do certyfikacji, w zakresie zgodności z przepisami RODO będzie Prezes Urzędu Ochrony Danych Osobowych. W planach Ministerstwa Cyfryzacji Prezes urzędu będzie opracowywał i udostępniał kryteria certyfikacji. UODO zastrzega sobie również możliwość przeprowadzenia czynności sprawdzających u administratora lub podmiotu przetwarzającego w okresie obowiązywania certyfikacji. Czynności sprawdzające będą mogły dotyczyć oceny spełniania przez certyfikowany podmiot kryteriów certyfikacji. Warto zauważyć, iż w wypadku gdy podczas czynności sprawdzających pojawią się nieprawidłowości Urząd będzie mógł wydać decyzję o cofnięciu certyfikacji. W naszej opinii przeprowadzenie przez UODO jako jedynego urzędu procesu certyfikacji zgodności operacji przetwarzania danych z przepisami RODO jest rozwiązaniem doprowadzającym do konfliktu interesów.
2) Każdy podmiot w ramach wewnętrznego systemu ma określić kryteria i metody potrzebne do zapewnienia skutecznej ochrony danych. Doprecyzowanie w proponowanym akcie wykonawczym jednolitych kryteriów, zakresu informacji oraz wskaźników monitorowania i mierzenie daje min. możliwość przejrzystości i porównywalności.
3) W związku z wprowadzeniem znowelizowanych przepisów dotyczących ochrony danych osobowych proponuje się wprowadzenie działań edukacyjnych dla społeczeństwa oraz mediów w zakresie ochrony danych osobowych. Ważne jest aby budowanie świadomości społeczeństwa odnośnie ochrona danych osobowych przyczyniło się do systematycznego eliminowania i unikania zdarzeń niepożądanych dotyczących danych a nie przekazywania społeczeństwu sensacyjnych informacji.
4) Rozdział 2 Inspektorzy ochrony danych
   - Należy doprecyzować, w jaki sposób mają być realizowane zadania inspektora ochrony danych, w szczególności wynikające z art. 39 ust. 1 pkt d i e Rozporządzenia 2016/679 (współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem). Dotychczas zasady współpracy pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych a administratorami bezpieczeństwa informacji wynikały wprost z Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zgodnie z art. 19b GIODO może zwrócić się do administratora bezpieczeństwa informacji o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami. Zasady prowadzenia sprawdzeń zostały ponadto określone w Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji. Podobnych regulacji, określających zasady współpracy pomiędzy inspektorem ochrony danych a organem nadzorczym, nie zawiera Rozporządzenie UE 2016/679 ani proponowane przepisy krajowe. Kwestia ta nie została również wyczerpująco rozwinięta w Wytycznych dotyczących inspektorów ochrony danych ('DPO') przyjętych w dniu 13 grudnia 2016 r. przez Grupę roboczą art. 29 ds. Ochrony danych.
     Ponadto zgodnie z Propozycją procedur postępowania przed GIODO –wypracowaną przez Zespół do spraw reformy prawa ochrony danych osobowych w Unii Europejskiej powołany Zarządzeniem nr 20/2016 Generalnego Inspektora Ochrony Danych z dnia 8 lipca 2016 r.,

Stowarzyszenie *Polska Unia Szpitali Klinicznych*
REGON: 140544131
NIP: 5272520070

Adres do korespondencji
ul. Długa 1/2, 61-848 Poznań
e-mail: uniaszpitali@skpp.edu.pl

stan prawny na 27 stycznia 2017 r. – w postępowaniu przed GIODO organ może zwrócić się do inspektora ochrony danych wyznaczonego przez administratora lub podmiot przetwarzający o udzielenie informacji w kwestiach związanych z przetwarzaniem danych przez tego administratora lub przez ten podmiot przetwarzający. Informacja taka stanowi dowód w postępowaniu. Co prawda przepisy rozporządzenia 2016/679 nie przewidują możliwości wprowadzenia przez państwa członkowskie szczególnych regulacji w zakresie statusu i zadań inspektora ochrony danych, ale zasady współpracy pomiędzy inspektorem a organem nadzorczym– zgodnie z powyższym przykładem – można uregulować także w przepisach dotyczących poszczególnych procedur postepowania.

- Zgodnie z projektowanym art. 5 ust. 6 ustawy Prezes Urzędu prowadzi wewnętrzną ewidencję zawiadomień o wyznaczeniu inspektora ochrony danych. Obecnie, zgodnie z art. 46c. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Generalny Inspektor Ochrony Danych Osobowych prowadzi ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji. Względy praktyczne przemawiają za utrzymaniem jawności rejestru.

5) Rozdział 5 Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych i Rozdział 7 Postepowanie kontrolne

- Zgodnie z art. 48 projektu ustawy o ochronie danych osobowych, prawo Prezesa Urzędu do dostępu do wszelkich informacji, w tym danych osobowych, niezbędnych Prezesowi Urzędu do realizacji zadań podlega ograniczeniu ze względu na tajemnice ustawowo chronione. Wykonywanie ww. prawa jest możliwe na zasadach określonych w przepisach regulujących dostęp do tajemnic ustawowo chronionych.

  W tym kontekście, należy jednoznacznie określić, czy i w jakim zakresie Prezes Urzędu powinien mieć dostęp do danych zawartych w dokumentacji medycznej, np. w toku prowadzonej kontroli i postępowań, z uwzględnieniem, że zgodnie § 8. Rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania w dokumentacji indywidualnej wewnętrznej zamieszcza się lub dołącza do niej:

  1) oświadczenie pacjenta o upoważnieniu do uzyskiwania informacji o jego stanie zdrowia i udzielonych świadczeniach zdrowotnych, ze wskazaniem imienia i nazwiska osoby upoważnionej oraz danych umożliwiających kontakt z tą osobą;
  2) oświadczenie pacjenta o upoważnieniu do uzyskiwania dokumentacji, ze wskazaniem imienia i nazwiska osoby upoważnionej.
  W przypadku przyznania takiego uprawnienia, powinno to znaleźć odzwierciedlenie w art. 26 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Podobnie na mocy nowelizacji ww. ustawy z dnia 23 marca 2017 r. przeredagowano przepis art. 26 ust. 3 pkt 2, aby w sposób jednoznaczny wynikało z niego uprawnienie Rzecznika Praw Pacjenta do dokumentacji medycznej.

Podobne rozstrzygnięcia należy podjąć w stosunku do osoby upoważnionej przez Prezesa Urzędu do przeprowadzenia kontroli. Zgodnie z projektowanym art. 69 ust. 1 pkt 2 w celu uzyskania informacji mogących stanowić dowód w sprawie kontrolujący ma prawo wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli. Należy jednoznacznie określić, czy kontrolerzy mogą przetwarzać dane, o których mowa w art. 9 rozporządzenia 2016/679, w szczególności czy powyższe uprawnienie obejmuje dostęp do dokumentacji medycznej. Podobna regulacja znalazła się w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli. Zgodnie z art. 29 ust. 1 pkt 2 ppkt b ww. ustawy upoważnieni przedstawiciele Najwyższej Izby Kontroli mają prawo do wglądu do wszelkich dokumentów związanych z działalnością jednostek kontrolowanych, pobierania oraz zabezpieczania dokumentów i innych materiałów dowodowych, z zachowaniem przepisów o tajemnicy ustawowo chronionej, dodatkowo ppkt i określa prawo kontrolerów do przetwarzania danych osobowych, z wyjątkiem danych ujawniających poglądy polityczne, przekonania religijne lub filozoficzne, jak również danych o kodzie genetycznym, nałogach lub życiu seksualnym.

- Zgodnie z projektowanym art. 57 ust. 3 organy, o których mowa w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego a także podmioty publiczne, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, niezwłocznie udostępniają na swoich stronach internetowych informacje o działaniach podjętych w celu wykonania decyzji Prezesa Urzędu, które mogą m.in. nakazywać administratorowi danych dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679.

  Udostępnianie powyższych informacji powinno następować z uwzględnieniem ograniczeń określonych w przepisach art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, tak samo jak zostało to przewidziane w stosunku do udostępnia samych decyzji Prezesa Urzędu.

  Należy wziąć pod uwagę, że ujawnienie stosowanych zabezpieczeń, może poważnie zagrozić bezpieczeństwu chronionych danych. Przez analogię można się tutaj powołać na orzecznictwo sądów administracyjnych dotyczące żądań udostępnienia dokumentów polityki bezpieczeństwa – zawierających m.in. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – na podstawie ustawy o dostępie do informacji publicznej (sygn. akt II SA/WA 1539/05; sygn. akt II SA/Wa 1135/15). Sądy przyjęły stanowisko, że polityka bezpieczeństwa nie powinna być udostępniana publicznie.

Uwagi dotyczące projektu ustawy - Przepisy wprowadzające ustawę o ochronie danych osobowych:

1. Art. 5 – zmiany w ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy

- Zgodnie z projektowanym art. 22^1 § 5 oraz art. 22^2 § 1 i 2 Kodeksu pracy przesłanką legalizującą przetwarzanie danych osobowych pracownika niewymienionych w art. 22^1 § 1 i 2, danych biometrycznych oraz adresu do korespondencji i adresu poczty elektronicznej albo numeru telefonu podanych w procesie rekrutacji ma być zgoda pracownika. Pomimo zawartego w art. 22^2 §3 zastrzeżenia, że brak zgody na przetwarzanie dodatkowych danych, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, dobrowolność wyrażania zgody przez pracownika budzi wątpliwości. W tej kwestii wypowiedział się również Naczelny Sąd Administracyjny, który w wyroku sygn. I OSK 249/09 stwierdził, że „wyrażona na prośbę pracodawcy pisemna zgoda pracownika, na pobranie i przetworzenie jego danych osobowych, narusza prawa pracownika i swobodę wyrażenia przez niego woli. Za tak sformułowanym stanowiskiem przemawia zależność pracownika od pracodawcy. Brak równowagi w relacji pracodawca pracownik stawia pod znakiem zapytania dobrowolność w wyrażeniu zgody na pobieranie i przetworzenie danych osobowych ..."
  Zgoda na przetwarzanie dodatkowych danych może dotyczyć czynności faktycznie dobrowolnych, jak np. zamieszczenie wizerunku pracownika na stronie internetowej lub identyfikatorze., nie zaś procesów obowiązkowych, jak prowadzenie ewidencji czasu pracy. W związku z powyższym należy wyłączyć możliwość stosowania zgody jako podstawy przetwarzania danych osobowych pracownika w celu wypełniania obowiązku pracodawcy nałożonego przepisem prawa, które nie są w tym celu niezbędne.

  Jeżeli dodatkowe dane są niezbędne do wypełniania obowiązku nałożonego przepisem prawa, pracodawca będzie mógł je pozyskać na podstawie art. 22^3, jeżeli nie są niezbędne, to zgodnie z zasadą adekwatności wyrażoną w art. 5 ust. 1 pkt c Rozporządzenia 2016/679 nie powinien ich przetwarzać.

  Wprowadzenie art. 22^2 § 1 i 2 bez dodatkowych zastrzeżeń może doprowadzić do obchodzenia przez pracodawców przepisów Kodeksu Pracy i pozyskiwania danych nadmiarowych w stosunku do celu, co jest wysoce ryzykowne w szczególności w odniesieniu do danych biometrycznych.

- Dodatkowo należy rozważyć relację między zaproponowanymi przepisami: zgodnie z art. 22^2 § 1. przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 22^1 § 1 i 2 jest dopuszczalne **tylko wtedy**, gdy dotyczą one stosunku pracy i osoba ubiegająca się o zatrudnienie lub pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej.

  Następujący dalej przepis art. 22^3§ 1 stanowi z kolei, iż pracodawca żąda podania m.in. danych osobowych innych niż określone w art. 22^1 § 1 i 2, jeżeli obowiązek ich podania wynika z

odrębnych przepisów lub gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa. Oznacza to, że przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 22^1 § 1 i 2 jest dopuszczalne **nie tylko wtedy**, gdy pracownik wyrazi na to zgodę, ale również wtedy, gdy wymagają tego przepisy prawa.

- Proponowane zmiany Kodeksu Pracy dopuszczają możliwość wprowadzenia przez pracodawcę monitoringu w miejscu pracy, przy czym w dalszym ciągu brak jest kompleksowej regulacji, określającej zasady prowadzenia monitoringu. W związku z powyższym w projektowanych przepisach Kodeksu Pracy należy zawrzeć wytyczne dotyczące realizacji praw osób objętych monitoringiem, w tym prawa do poprawiania/ usuwania danych oraz obowiązków administratora danych, w tym obowiązku informacyjnego wynikającego z art. 13 Rozporządzenia i jednoznacznie określić, czy powyższe prawa i obowiązki podlegają ograniczeniu ze względu na okoliczności gromadzenia danych, stosowaną technologię i postać danych.

  Jednocześnie zwracamy uwagę, że najlepszym rozwiązaniem byłoby przygotowanie ustawy całościowo regulującej zagadnienia związane z monitoringiem wizyjnym.

2. Zgodnie z art. 53. w ustawie z dnia 27 lipca 2001 r. o kuratorach sądowych administrator danych jest obowiązany udostępnić kuratorowi zawodowemu dane osobowe również w zakresie dotyczącym stanu zdrowia.

   Koniecznie jest uszczegółowienie informacji, o jakie może zwracać się kurator zawodowy w zakresie stanu zdrowia. W przeciwnym razie będzie to musiała być za każdym razem indywidualna decyzja administratora danych (podmiotu leczniczego). Jednoznacznego określenia wymaga, czy kurator jest uprawniony do uzyskania dokumentacji medycznej.

3. Zgodnie z art. 142 oraz 143 dane zgromadzone w rejestrze zbiorów danych osobowych oraz rejestrze administratorów bezpieczeństwa prowadzonych przez Generalnego Inspektowa Ochrony Danych Osobowych, Prezes Urzędu przechowuje przez okres 3 lat od dnia wejścia w życie niniejszej ustawy. Należy określić, sposób postępowania z powyższymi danymi po upływie okresie przechowywania wskazanego w powyższych przepisach. Ustalenia wymaga, czy dane powinny zostać zniszczone, zwrócone administratorom danych, czy też zostaną uznane za materiał archiwalny w rozumieniu przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach i będą podlegać przepisom tejże ustawy.