KRASP

www.krasp.org.pl

Konferencja Rektorów Akademickich Szkół Polskich

Przewodniczący:

prof. dr hab. inż. Jan Szmidt
Rektor
Politechniki Warszawskiej
president@krasp.org.pl

Biuro KRASP:

Krakowskie Przedmieście 26/28
00-927 Warszawa
tel.: 22 55 20 352
fax: 22 55 21 567
biuro@krasp.org.pl

Warszawa, 16 października 2017 r.

KRASP/364/2017

Szanowna Pani
Anna Streżyńska
Sekretarz Stanu
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowna Pani Minister,

w odpowiedzi na pismo z nr DP.WLI.0211.2017 z 14 września 2017 r. w załączeniu przekazuję uwagi Komisji ds. Organizacyjnych i Legislacyjnych oraz Komisji ds. Infrastruktury Informatycznej Konferencji Rektorów Akademickich Szkół Polskich dotyczące projektu ustawy o ochronie danych osobowych oraz projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych.

Z wyrazami szacunku,

Prof. dr hab. inż. Jan Szmidt
Przewodniczący KRASP

14 października 2017 r.

Uwagi
Komisji ds. Organizacyjnych i Legislacyjnych
oraz
Komisji ds. Infrastruktury Informatycznej
Konferencji Rektorów Akademickich Szkół Polskich
dotyczące
projektu ustawy o ochronie danych osobowych oraz projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych
(projekty z dn. 12 września 2017 r.)

Projekt z dnia 12 września 2017 r. nowej ustawy o ochronie danych osobowych wynika z konieczności wdrożenia do polskiego systemu prawnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „Rozporządzeniem" lub „RODO".

Należy zauważyć, że Rozporządzenie będzie obowiązywało w polskim porządku prawnym bezpośrednio i stosowane będzie od dnia 25 maja 2018 r., w związku z czym polskie przepisy muszą zapewniać skuteczne stosowanie Rozporządzenia, przy czym regulacje prawa polskiego nie mogą być sprzeczne z Rozporządzeniem i nie powielać jego rozwiązań. Podstawową różnicą między Rozporządzeniem a dyrektywą, która je poprzedza (95/46/WE), jest brak potrzeby implementacji nowych przepisów do krajowego porządku prawnego, a więc będzie stosowane wprost. Oznacza to, że przepisy nowej ustawy o ochronie danych osobowych nie będą regulować zagadnień materialno-prawnych, a ustrojowe i proceduralne – w szczególności unormowanie pozycji prawnej i uprawnień organu nadzorczego oraz procedury postępowania.

W polskim ustawodawstwie ochrona informacji o osobach fizycznych znajduje swoje umocowanie w Konstytucji RP w art. 47 i 51, które wprowadzają prawo do ochrony życia prywatnego oraz prawo obywateli do kontrolowania gromadzenia informacji na ich temat. Zasady, o których mówi Konstytucja, dotychczas unormowane były ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, która do polskiego porządku prawnego implementowała wspomnianą wyżej dyrektywę 95/46/WE, tak więc prawo do ochrony danych osobowych jest zaliczane do prawa publicznego – w polskim systemie prawnym traktowane jest jako element systemu prawa administracyjnego.

ANALIZA PROJEKTU NOWEJ USTAWY O OCHRONIE DANYCH OSOBOWYCH

Rozdział 1 projektu nowej ustawy o ochronie danych osobowych wskazuje zakres przedmiotowy i podmiotowy. Zgodnie z treścią art. 1 ust. 1 ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i 3 RODO. Oznacza to, że ochrona danych powinna mieć zastosowanie do osób fizycznych, bez względu na obywatelstwo czy miejsce zamieszkania. Należy zauważyć, że ochrona danych nie będzie dotyczyła osób prawnych, w szczególności przedsiębiorstw

będących osobami prawnymi, w tym danych o firmie. Zakres przedmiotowy obejmuje przetwarzanie danych w sposób całkowicie zautomatyzowany, częściowo zautomatyzowany, a także dotyczy przetwarzania w sposób inny niż zautomatyzowany. Przepis art. 1 ust. 1 jest zgodny z treścią Rozporządzenia także w kwestii dot. terytorialnego zakresu stosowania, a mianowicie ustawa będzie miała także zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii czy poza Unią. Ma także ma zastosowanie do przetwarzania danych osobowych osób przebywających w Unii, których dane te dotyczą, przez administratora lub podmiot przetwarzający niemający jednostek organizacyjnych w Unii, jeżeli przetwarzanie wiąże się z oferowaniem towarów lub usług takim osobom czy monitorowaniem ich zachowania. Nowa ustawa pozwala także na stosowanie jej w przypadku przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Bliżej natomiast należy przyjrzeć się treści art. 2 ust. 1 i 2, który w ust. 1 dotyczy działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu materiałów prasowych w rozumieniu ustawy Prawo prasowe, a także do działalności literackiej lub artystycznej, a w ust. 2 wypowiedzi akademickiej. Celem ww. artykułu jest wyłączenie spod stosowania przepisów rozporządzenia czynności określonych w zdaniu poprzednim. O ile za słuszne należy uznać chęć wyłączenia spod stosowania przepisów Rozporządzenia ww. aktywności, to wątpliwość nasuwa zamiana słowa „wypowiedź", którym posługuje się RODO, a które nie jest znane polskiemu prawodawcy tylko w odniesieniu do wypowiedzi artystycznej i literackiej na działalność artystyczną i działalność literacką, natomiast pozostawienie wypowiedzi akademickiej. W uzasadnieniu projektodawca twierdzi, że pojęcie działalności w odniesieniu do aktywności artystycznej i literackiej jest tożsame z pojęciem „wypowiedzi", które to aktywności mogą być wyrażone w określonej formie, natomiast „wypowiedź akademicka" „stanowi tylko jeden z elementów działań podejmowanych przez uczelnie wyższe" – a przecież zarówno działalność artystyczna jak i działalność literacka nie obejmują tylko „wyrażenia w określonej formie"; to także szereg działań podejmowanych w jakimś celu, a także funkcjonowanie i oddziaływanie na coś. Termin wypowiedź ma natomiast dużo węższą konotację i odnosi się do ustnego lub pisemnego zabrania głosu w jakiejś sprawie. Konieczne zatem wydaje się doprecyzowanie, jaki charakter zgodnie z przepisami o ochronie danych osobowych może przyjmować „wypowiedź akademicka", by można było zastosować wyłączenie, o którym mowa w art. 2 ust. 2 projektu ustawy o ochronie danych osobowych, zwłaszcza gdy również Rozporządzenie nie definiuje pojęcia wypowiedzi akademickiej.

W zakresie art. 4 należy zwrócić uwagę na zapis budzący wątpliwość co do tego, kiedy ma nastąpić notyfikacja (a wcześniej powołanie) ze strony Administratora Danych (dotycząca Inspektora Ochrony Danych) do organu nadzorczego – w kontekście wejścia w życie ustawy. Aby zapewnić legalność swojego działania na dzień 25 maja 2018 r. administrator danych winien raczej powołać inspektora przed dniem wejścia w życie ustawy (najpóźniej zaś 25 maja). Wówczas na zawiadomienie organu pozostawać będzie 14 dni, a ww. notyfikacja mieć będzie wyłącznie charakter deklaratywny. W tej sytuacji wskazać należy, że termin 30-dniowy na notyfikację nie byłby przesadnie długi, a z uwagi na wielość zadań i obowiązków osób reprezentujących administratora danych termin taki byłby łatwiejszy do dotrzymania. Brak charakteru konstytutywnego takiej notyfikacji świadczy też o tym, że stosunkowo krótki 14-dniowy termin nie wydaje się uzasadniony.

W przypadku zapisów art. 5 ust. 4 pożyteczne wydaje się doprecyzowanie – w sytuacji gdy podpis kwalifikowany lub Profil Zaufany ma mieć zastosowanie do tej czynności - kto konkretnie może notyfikować IOD w sytuacji gdy administratorem danych jest organizacja, którą reprezentuje nie konkretna osoba, a organ – np. zarząd fundacji; w szczególności, czy notyfikacji może dokonać sam IOD powołany na pełnomocnika takiej organizacji ds. danych osobowych lub w inny - podobnie ogólnikowy - sposób.

W art. 5 ust. 5, ale też w wielu innych miejscach, ustawodawca traktuje o „systemie teleinformatycznym". Wskazane jest zapytanie, czy będzie to inny system niż skrzynka ePUAP urzędu/organu/Prezesa.

Odnośnie do art. 5 ust. 6, zasadne wydaje się zadanie pytania, dlaczego ewidencja zawiadomień ma mieć charakter wewnętrzny, skoro z mocy samego RODO administrator ma obowiązek wypełniać obowiązek informacyjny z podawaniem nazw (nazwisk) oraz danych kontaktowych administratorów (i ich przedstawicieli) i - tak samo - powołanych przez siebie IOD? Czy nie byłoby rozsądne udostępnienie tych danych prowadzonych w rejestrze organu publicznego do wiadomości powszechnej, tak aby administrator danych mógł wykonywać obowiązek informacyjny wskazując po prostu na dane ujawnione przez niego i wprowadzone do tej ewidencji. Byłoby to szczególnie pomocne w sytuacji, gdyby miało dojść (a nawet dochodzić wielokrotnie) do zmiany osoby pełniącej funkcje IOD, a każdorazowe zawiadamianie o tej zmianie wszystkich osób, których dane dotyczą, byłoby po prostu nadmiernie uciążliwe.

Rozdział 3 komentowanego projektu ustawy dotyczy certyfikacji i akredytacji. Jest to nowość w tematyce ochrony danych osobowych, która dotychczas nie występowała w przepisach o ochronie danych. Głównym celem uzyskania certyfikatów i akredytacji jest ułatwienie podmiotom publicznym (przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw) wdrożenia zasad ochrony danych osobowych, a przede wszystkim przygotowanie właściwych kodeksów postępowania. Rozporządzenie pozostawia ustawodawcy swobodę co do wyboru właściwego organu nadzorczego. Projektodawca zdecydował, że podmiotem, który będzie uprawniony do działań certyfikacyjnych, jest Prezes Urzędu Ochrony Danych Osobowych. W art. 8 ust. 1 projektowanej ustawy - mimo iż byłoby to powtórzenie z treści art. 42 Rozporządzenia - wskazana jest mała modyfikacja treści, a mianowicie art. 8 ust. 1 powinien uzyskać brzmienie: „Certyfikacja jest dobrowolna, dokonuje się na wniosek administratora lub podmiotu przetwarzającego". Kwestią, która nie budzi wątpliwości jest kwestia dotycząca podmiotów akredytowanych (art. 17 projektu ustawy).

Art. 7 projektowanej ustawy mówi, iż Prezes Urzędu opracowuje kryteria certyfikacji i udostępnia je w BIP. Wypada zastanowić się, czy kryteria, o których mowa w art. 7, powinny być publikowane tylko w BIP, czy raczej nie powinny uzyskać rangi co najmniej rozporządzenia, a także, czy kryteria będą stałe czy zmienne w zależności od podmiotu przetwarzającego dane osobowe, a także czy będą one przewidywać wszystkie możliwe operacje przetwarzania danych. W świetle Rozporządzenia administrator danych ma podejmować działania polegające na analizie ryzyka, a także na zapewnieniu domyślnej ochrony danych, rodzi się więc pytanie, czy kryteria będą pozostawiać pewną dowolność w wyborze środków ochrony danych.

W art. 12 wspomina się o publicznie dostępnym wykazie administratorów i podmiotów przetwarzających (ale w odniesieniu do tych, którym udzielono certyfikacji). Z technicznego punktu widzenia prowadzenie takiego wykazu także dla podmiotów niecertyfikowanych nie powinno nastręczać problemu.

W art. 13 ust. 1 zaproponować wypada dodanie po słowach: „... po udzieleniu certyfikacji" słów: „jednakże nie później niż do końca okresu objętego certyfikacją". W art. 13 ust. 2 po słowie „...zawiadamia" wskazane jest dodanie (celem doprecyzowania): „indywidualnie, pisemnie administratora lub podmiot przetwarzający".

Odnośnie do art. 17 należy zauważyć, że KRASP wydaje się być właściwą organizacją do tego, by jako organ reprezentatywny dla środowiska akademickiego, ubiegać się o odpowiednią certyfikację, a następnie dbać o przestrzeganie zatwierdzonego kodeksu postępowania mającego zastosowanie w uczelniach publicznych.

Kluczowa dla nowej ustawy o ochronie danych osobowych jest regulacja dot. Prezesa Urzędu Ochrony Danych Osobowych (Rozdział 4). Z prawnego punktu widzenia następcą prawnym Generalnego Inspektora Ochrony Danych Osobowych będzie Prezes Urzędu Ochrony Danych Osobowych. Zmiana taka wynika z przepisów Rozporządzenia i uzasadniana jest wprowadzeniem Inspektorów Ochrony Danych. Warto także zwrócić uwagę, iż pracownicy GIODO nazywani są inspektorami, co mogłoby powodować pewną sprzeczność interpretacyjną. Jedynym argumentem przemawiającym za pozostawieniem dotychczasowej nazwy, który podnoszony był także przez GIODO na szkoleniu dla ABIch w listopadzie 2016 r. i konferencji poświęconej ochronie danych osobowych z dnia 22 września 2017 r. byłoby to, iż GIODO wypracowało sobie już pewną markę i status jako organ, a w związku z nowymi przepisami może dojść do sytuacji, że nowy podmiot będzie na nowo musiał budować swój status. Przepisy dot. powołania Prezesa Urzędu Ochrony Danych Osobowych spełniają wymagania określone w Rozporządzeniu i nie budzą wątpliwości co do zapewnienia niezależności urzędu.

Za prawidłowe działanie projektodawcy należy uznać przyznanie Prezesowi Urzędu kompetencji dot. nadawania statutu Urzędu, który określa organizację Urzędu, zakres zadań zastępców oraz zakres zadań i tryb pracy komórek organizacyjnych Urzędu. W obowiązującej ustawie o ochronie danych osobowych statut nadawany był przez Prezydenta RP po zasięgnięciu opinii GIODO.

W art. 20 ust. 4 wątpliwości zdaje się budzić sposób określenia kompetencji czy też wymagań stawianych osobie ubiegającej się o stanowisko Prezesa Urzędu. Ogólne określenie wymogu „posiadania tytułu naukowego doktora" bez powiązania z jakąś konkretną dziedziną nie gwarantuje, że osoba taka będzie miała przymioty niezbędne do wykonywania tych zadań. Ze względu na specyfikę przedmiotu czy powinno się wykluczać, że praktyk posiadający wykształcenie wyższe – prawnik, urzędnik lub informatyk może mieć lepsze przygotowanie do wykonywania tej funkcji.

W tym samym punkcie wskazane jest rozważenie, czy Prezes urzędu nie podlega także przepisom UE, w szczególności zaś przepisom Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

W odróżnieniu od obowiązującej jeszcze ustawy o ochronie danych osobowych, gdzie zastępca GIODO powoływany jest na wniosek Generalnego Inspektora Danych przez Marszałka Sejmu, art. 22 projektowanej ustawy mówi, iż Prezes Urzędu wykonuje swoje zadania przy pomocy trzech zastępców, dwóch powoływanych jest na wniosek ministra właściwego do spraw informatyzacji, a jednego na wniosek ministra właściwego do spraw wewnętrznych przez Prezesa Rady Ministrów. Oznacza to, że najbliżsi współpracownicy Prezesa Urzędu będą mu narzuceni niejako z góry, co w pewnym sensie może wpływać na jego niezależność dot. np. kwestii kształtowania polityki dot. nadzoru, a także może mieć wpływ na upolitycznienie Urzędu.

W art. 23 nieco niejasne wydaje się użycie słów „wykonywanie innych zajęć zarobkowych i niezarobkowych sprzecznych z obowiązkami Prezesa". Nie eliminuje to ewentualnego konfliktu interesów, który może zaistnieć w tym układzie ról, jaki przedstawia projekt ustawy. Poza tym nadmiernie ocenne i podatne na interpretacyjne rozbieżności jest określenie „działalność nie dająca się pogodzić z godnością urzędu".

Odnośnie do art. 34 ust. 6 za wskazane należy uznać, aby kandydatów do Rady wskazywały podmioty określone w ust. 7. Nie byłoby złym rozwiązaniem, aby miejsca w radzie przypisane były właśnie do tych podmiotów i aby miały one (a szczególnie RPO) zagwarantowaną możliwość obsadzenia tego miejsca jednym z wytypowanych przez siebie kandydatów. W przypadku powołania się na definicję z ustawy o finansowaniu nauki (art. 34 ust. 7 pkt 8) należy przypomnieć o wątpliwej przyszłości tej ustawy w kontekście prac nad Ustawą 2.0. Czy nie należałoby określić wprost organizacji reprezentatywnych dla jednostek naukowych – np. KRASP?

Art. 39 ust. 1 w projektowanym brzmieniu dotyczy tylko „wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych". Czy jednak wobec mało dotąd upowszechnionej konstrukcji ogólnego „wykazu rodzajów operacji przetwarzania" Prezes nie powinien zostać zobligowany do publikowania także wykazu operacji przetwarzania danych, o którym mowa w art. 35 ust. 5 (czyli nawet wtedy gdy „nie podlega wymogowi dokonywania oceny skutków")?

W art. 43 ust. 3 wskazane jest dookreślenie trybu konsultacji.

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych w projekcie nowej ustawy odnosi się do naruszeń wynikających z tejże ustawy i RODO. Prowadzone jest ono według norm określonych Kodeksem postępowania administracyjnego, o ile przepisy nie stanowią inaczej. Postępowanie ma charakter jednoinstancyjny. Decyzje wydawane przez Prezesa Urzędu będą ostateczne i nie będzie możliwe złożenie wniosku o ponowne rozpoznanie sprawy, a tylko złożenie skargi do sądu administracyjnego. Zastosowanie trybu jednoinstancyjnego w ocenie projektodawcy ma na celu przyśpieszenie wykonalności decyzji i szybkość reakcji na ew. naruszenie ochrony danych osobowych. Warto zauważyć, że wprowadzenie trybu jednoinstancyjnego stanowi wyjątek od zasady dwuinstancyjności. Wydaje się, że pozbawienie możliwości złożenia wniosku o ponowne rozpatrzenie sprawy może powodować skutki, które mogą być dotkliwe dla podmiotu, dla którego decyzja stała się ostateczna. Pozbawia to ten podmiot możliwości podjęcia konkretnych działań przed ponownym rozpoznaniem. Uzasadnienie podane przez projektodawcę może tak naprawdę odnosić się do dowolnej decyzji wydawanej w toku postępowania, zasadne wydaje się więc podanie przez projektodawcę szczególnej celowości rezygnacji z trybu dwuinstancyjnego. Jest to bardzo rygorystyczna koncepcja, której realizacja w praktyce może prowadzić do

nieodwracalnych skutków dla przedsiębiorców i stanowić poważne ograniczenie w zakresie realizacji ich prawa do skutecznego środka odwoławczego.

W art. 50 ust. 1 zamiast „lub innych tajemnic podlegających ochronie na podstawie odrębnych przepisów" należałoby raczej napisać „lub innych tajemnic ustawowo chronionych".

Art. 50 ust. 2 wprowadza pojęcie „wersji dokumentu". Nie jest jednak określone, co to znaczy Możliwe jest, że dokument bez pewnych "metadanych" przestaje w zasadzie być dokumentem (nie zawiera treści, które miałby potwierdzać). Jak trzeba będzie rozumieć zatem integralność takiej „wersji" dokumentu?

W odniesieniu do art. 53 - z uwagi na wagę sankcji w postaci ograniczenia przetwarzania danych wydaje się niezbędne zapewnienie stronie czynnego udziału (wypowiedzenia się o zakresie ograniczenia przetwarzania). Prezes Urzędu nie może znać specyfiki każdego rodzaju przetwarzania, a odebranie głosu stronie, której często „być albo nie być" zależy od przetwarzania danych nie znajduje dostatecznego uzasadnienia, tym bardziej że § 2 w art. 10 k.p.a. przewiduje już określone okoliczności odstąpienia od tej zasady.

W odniesieniu do art. 55 ust. 1 należy zapytać o to, jaką formę będzie mieć „wydanie ostrzeżenia", o którym mowa w art. 58 ust. 2 lit. a); czy Prezes będzie mógł wydawać takie ostrzeżenie na podstawie jedynie tylko tego przepisu Rozporządzenia?

Proponowana treść art. 57 zdaje się wprowadzać nieuzasadnione wyłączenie; jaki bowiem może być powód wyłączenia z udostępnienia w BIP informacji o:
„h) cofnięciu certyfikacji lub nakazaniu podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
i) zastosowaniu, oprócz lub zamiast środków, o których mowa w niniejszym ustępie, administracyjnej kary pieniężnej na mocy art. 83, zależnie od okoliczności konkretnej sprawy;"
Dlaczego cofnięcie certyfikacji (a nawet zastosowanie kary pieniężnej) miałoby nie być już informacją publiczną?

Rozdział 7 projektu ustawy skupia się na kryteriach dot. postępowania kontrolnego prowadzonego przez Prezesa Urzędu. Zgodnie z projektem nowej ustawy kontrola ma być prowadzona przez upoważnionego pracownika Urzędu Ochrony Danych zwanego „kontrolującym". Nowością jest możliwość prowadzenia kontroli pod nieobecność kontrolowanego – wystarczające ma być okazanie upoważnienia do przeprowadzenia kontroli pracownikowi kontrolowanego lub przywołanemu świadkowi, którym powinien być funkcjonariusz publiczny.

W świetle projektowanego przepisu (art. 68 ust. 2) wydaje się, że dostęp do jednostek kontrolowanych będzie w zasadzie nieograniczony, zwłaszcza że w art. 69 zrezygnowano z oznaczenia czasu na przeprowadzenie kontroli w godzinach 6.00 – 22.00. Tak więc ustawodawca pozwala organowi kontrolnemu na prowadzenie kontroli w sposób prowadzony przez organy ścigania, zwłaszcza że procedura kontrolna może odbywać się przy udziale organów kontroli państwowej lub Policji. Nie wydaje się zasadne, aby prowadzenie postępowania kontrolnego w zakresie naruszenia ochrony danych osobowych wymagało posługiwania się służbami mundurowymi państwa, a także wymagało dostępu do organu

kontrolowanego w godzinach innych niż wskazane w obowiązującej ustawie o ochronie danych osobowych.

Art. 68 ust. 2 oraz art. 72 ust. 3 wydają się być ze sobą w sprzeczności, bo kto może podpisać protokół kontroli w sytuacji, gdy administrator danych lub upoważniona przez niego osoba była nieobecna. Czy podpis pracownika, którego wybrał kontrolujący bądź świadka będącego organem administracji publicznej uczestniczącego w postępowaniu kontrolnym będzie zgodny z prawem? Administrator danych czy osoba przez niego upoważniona nie będą mieli możliwości zweryfikowania, czy faktycznie kontrola przetwarzania danych odbywała się zgodnie z przyjętymi ustawowo normami.

Zdecydowanie negatywnie należy podejść również do uregulowań dotyczących postępowania kontrolnego przeprowadzanego przez PUODO, które nie chroni przedsiębiorców przed jego nadmierną uciążliwością. Ustawodawca przewidział wyłączenia od zawiadamiania o zamiarze kontroli oraz wyłączenia przepisów ograniczających czas trwania kontroli przewidziane w ustawie o swobodzie działalności gospodarczej. Możliwe będzie też prowadzenie więcej niż jednej kontroli jednocześnie u przedsiębiorcy, w tym kontroli dotyczącej zapewnienia właściwej ochrony danych osobowych. Nie podważając potrzeby zapewnienia wysokiego poziomu ochrony danych osobowych, można mieć wątpliwości co do proporcjonalności przyjętych rozwiązań w kontekście zapewniania swobody działalności gospodarczej.

Administracyjne kary pieniężne nakładane na organy i podmioty publiczne wynikają z przesłanek ich nakładania wyrażonych w Rozporządzeniu. W świetle projektowanych przepisów de facto kary pieniężne będą nakładane tylko na podmioty publiczne. Nakładanie kar na podmioty publiczne, które są finansowane ze środków budżetu państwa mija się z celem, gdyż pieniądze te trafiałyby ponownie do budżetu państwa. Jeżeli celem projektodawcy była chęć zasilenia proponowanego Funduszu Ochrony Danych Osobowych, którego środki w 1% miałyby pochodzić z kar pieniężnych, to wprowadzenie tych przepisów mija się z celem, gdyż Urząd Ochrony Danych Osobowych finansowany z budżetu państwa i zgodnie z przepisami Rozporządzenia w ten sposób m.in. może realizować zadania o których mowa w art. 86 ust. 4.

ANALIZA PROJEKTU USTAWY PRZEPISY WPROWADZAJĄCE USTAWĘ O OCHRONIE DANYCH OSOBOWYCH

Projektodawca miał dwie możliwości dot. zmian w przepisach sektorowych: mógł uprzednio dokonać zmiany ustawy o ochronie danych osobowych, a następnie rozpocząć dostosowywanie pozostałych przepisów do treści nowej ustawy bądź - jak to zrobiono w przypadku omawianych dokumentów - rozpocząć pracę nad przepisami o ochronie danych osobowych i przepisów sektorowych równocześnie. Przyjęte rozwiązanie (projekt) zmienia przepisy 133 ustaw, a więc szereg ustaw pozostaje bez ingerencji w zmiany dot. ochrony danych osobowych.

Zmiany proponowane w ustawie o postępowaniu egzekucyjnym mają dwojaki charakter, pierwsza zmiana dot. tylko i wyłącznie zmiany organu właściwego w sprawach ochrony danych osobowych, natomiast projektowany art. 36 § 4 stanowi wyłączenie ze stosowania przepisów określonych w art. 12-22 i art. 34 Rozporządzenia. Zastosowanie takiego ograniczenia wydaje się adekwatne co do zakresu realizacji zadań publicznych przez organy egzekucyjne i wierzycieli.

Liczne zmiany zostały zaproponowane przez projektodawcę w zakresie ustawy Kodeks pracy. Jeżeli chodzi o proponowaną treść art. 221 w pełni odpowiada ona potrzebom przetwarzania danych osobowych przez pracodawcę na etapie zatrudnienia pracownika. Zwiększył się zakres przetwarzanych danych osobowych, a także zaostrzony został rygor dot. przetwarzania danych innych niż te, które wymienione są w art. 22 (ze zn.1), a mianowicie przetwarzanie danych osobowych innych dopuszczalne jest tylko wtedy, gdy dotyczą one stosunku pracy, a osoba, której dane dotyczą, wyrazi na to wyraźną zgodę Należy podnieść, że projektowany zapis art. 22 (ze zn.2) Kodeksu pracy może być sprzeczny z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – Rozporządzenie to bowiem w art. 9 pozwala przetwarzać dane biometryczne za wyraźną zgodą osoby, której te dane dotyczą, a projekt zmian do Kodeksu pracy tego zakazuje.

Istotną kwestią, którą porusza proponowany projekt, jest zapis dotyczący wprowadzenia szczególnego nadzoru nad miejscem pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Od wielu lat próbowano uregulować kwestię dotyczącą monitoringu, jednak do dnia dzisiejszego nie wprowadzono stosownych przepisów, a w kwestiach dot. monitoringu można było posłużyć się wytycznymi GIODO. Kwestia monitoringu CCTV wymaga regulacji, jednak tylko w odniesieniu do pracowników i pracodawcy nie spełnia pokładanych w regulacji nadziei.

Zmiana zaproponowana w ustawie o prawie autorskim i prawach pokrewnych polega na uregulowaniu kwestii dot. oświadczenia woli otrzymania wynagrodzenia za użyczenie, którą obecnie reguluje odrębne rozporządzenie. Regulacji poddano także zakres przetwarzania danych osobowych m.in. przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego czy organizacji zbiorowego zarządzania prawami autorskimi lub prawami pokrewnymi w celu realizacji ich zadań.

W ustawie o zakładowym funduszu świadczeń socjalnych proponuje się wprowadzenie zapisów legalizujących pobieranie danych osobowych w celu uzyskania ulgowej usługi i świadczenia.

Projektowana zmiana dot. bibliotek w dużej mierze określa zakres danych, jaki dla realizacji celów bibliotecznych biblioteka może przetwarzać.

Projekt ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych w art. 75 dotyczy uchylenia art. 88 ust. 5 ustawy Prawo o szkolnictwie wyższym. Z punktu widzenia uczelni zmiana przepisu, który dotyczy tylko rejestracji zbiorów danych przetwarzanych w systemach bibliotecznych nie jest wystarczająca - powinien pojawić się zapis mówiący, iż dane przetwarzane przez szkoły wyższe przetwarzane są do realizacji celów określonych w ustawie Prawo o szkolnictwie wyższym, a także powinno pojawić się wskazanie, że zgoda na przetwarzanie danych studentów nie jest wymagana do realizacji celów ustawowych.

Konieczne wydaje się doprecyzowanie kwestii prawa do bycia zapomnianym wynikającej z Rozporządzenia. Może dojść do sytuacji, gdy student lub doktorant otrzyma decyzję negatywną o przyjęciu na studia w związku z czym ma prawo żądać usunięcia jego danych ze zbiorów uczelni, a kwestia wyrażanej wcześniej zgody na przetwarzanie danych w celach

rekrutacyjnych mu na to pozwala. Dochodzi tutaj do styku z ustawą Kodeks postępowania administracyjnego, gdyż decyzja o odmowie przyjęcia na studia ma charakter decyzji administracyjnej i uczelnia nie może usunąć akt studenta, co do którego toczy się postępowanie administracyjne. Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego w sprawie dokumentacji przebiegu studiów nie reguluje tej kwestii, a wydaje się, że regulacje dot. przetwarzania danych studentów powinny zostać zawarte w akcie prawnym o charakterze ustawowym.

Kolejne wymagające uregulowania zagadnienie, którego zabrakło w projektowanych przepisach, dotyczy tego, czy szkoła wyższa może na wniosek osoby trzeciej (np. pracodawcy) bez zgody osoby, której dane dotyczą, udostępniać informacje o wykształceniu. O ile co do potwierdzenia np. autentyczności dyplomu nie ma problemu, to do szkoły wyższej wpływa wiele wniosków dot. stwierdzenia, czy dana osoba była jej studentem, co w przypadku potwierdzenia takiej informacji daje podstawy to naruszenia przepisów o ochronie danych osobowych. Z punktu widzenia szkoły wyższej istotnym zagadnieniem jest działanie na styku ustawy o ochronie danych osobowych i dostępie do informacji publicznych. Dlatego w ustawie Prawo o szkolnictwie wyższym powinien pojawić się zapis, mówiący o tym, iż dane studentów są przetwarzane w celu realizacji zadań określonych ustawą Prawo o szkolnictwie wyższym i nie podlegają udostępnieniu na podstawie przepisów o dostępie do informacji publicznej. W świetle projektowanych przepisów adekwatne wydaje się dodanie zapisu mówiącego, iż administratorem danych gromadzonych przez szkołę wyższą jest szkoła wyższa, a nie jej jednostki, co rozwiałoby wszelkie wątpliwości.

PODSUMOWANIE

Przepisy projektowanej ustawy o ochronie danych osobowych w dość sporym zakresie wpisują się w obowiązki wynikające z Rozporządzenia Parlamentu Europejskiego i Rady Europy, natomiast wyłączenie z pracy nad ustawą Generalnego Inspektora Ochrony Danych Osobowych, którego następcą ma zostać Prezes Urzędu Ochrony Danych należy uznać za nieuzasadnione. Proponowane przepisy ustrojowe w obecnym kształcie nie gwarantują niezależności organu, a rodzą niebezpieczeństwo potencjalnego konfliktu, jeżeli chodzi o niezależność organu. Konieczne wydaje się doprecyzowanie zagadnienia, jakim jest „wypowiedź akademicka". Jeżeli chodzi o zagadnienia dotyczące certyfikacji, to wypada się zastanowić, czy wymogi prawidłowego procesu certyfikacji wystarczy publikować na łamach BIP. Konotacja art. 1 ustawy powinna dotyczyć ochrony danych osobowych, a nie osób fizycznych. Zaniepokojenie budzą regulacje kontrolne, które uprawniają organ do prowadzenia kontroli nieograniczonych.

Regulacje dotyczące przepisów sektorowych nie powinny być wprowadzane w tym samym czasie co regulacje dotyczące ochrony danych osobowych. Zmiany w przepisach sektorowych wymagają konsultacji nie tylko na poziomie resortowym, ale przede wszystkim na poziomie podmiotów publicznych, które będą wykorzystywać przepisy w prowadzonej działalności. W związku z tym może pojawić się wiele innych sugestii i propozycji zmian przepisów, co znacznie wydłuży prace nad regulacjami sektorowymi. Zrozumiała jest chęć szybkiego wprowadzenia przepisów o ochronie danych do obowiązującego porządku prawnego, by dostosować przepisy do dnia 25 maja 2018 r., jednak w obecnym kształcie zmiany wydają się być przygotowane niedbale i bez porozumienia z Generalnym Inspektorem Ochrony Danych Osobowych czy innymi podmiotami przetwarzającymi dane osobowe.

Projekty nowych przepisów dotyczących ochrony danych osobowych, należy raczej określić jako „ewolucyjne". Są one dostosowywane do ukształtowanego już rynku cyfrowego. Za priorytetowe należy uznać przeprowadzenie audytu danych osobowych w jednostkach uczelni, przygotowanie regulacji o charakterze proaktywnym – zwłaszcza w zakresie dotyczącym analizy ryzyka już na etapie zbierania danych osobowych i przygotowania wytycznych co do zastosowania w działalności uczelni „domyślnej ochrony danych osobowych", w tym kwestii dotyczącej naruszeń ochrony danych osobowych. Konieczne wydaje się także ustalenie zakresu, w jakim ma być stosowany przepis Rozporządzenia mówiący o „prawie do bycia zapomnianym", a także uregulowanie uprawnienia do przenoszenia danych.

Można wyrażać oczekiwanie, że nowe przepisy będą zawierały urealnione zapisy dotyczące np. systemu POLON, administrowania czy współadministrowania tym systemem (czy systemem SL2014), właściwego zakresu danych (i przesłanek do ich przetwarzania) przy realizacji programów badawczych i w związku z finansowaniem nauki, awansem naukowym, procesem dydaktycznym etc. Zakres tych spraw wykracza jednak poza samo wprowadzenie przepisów opiniowanej ustawy.

Generalny Inspektor Ochrony Danych na konferencji w dniu 22 września 2017 r. zapowiedział przygotowanie i przedstawienie wytycznych dot. kwestii wdrożenia Rozporządzenia i przepisów o ochronie danych osobowych, zwłaszcza w zakresie klauzul przetwarzania danych osobowych czy warunków uzyskania certyfikacji. Po ukazaniu się takich wytycznych będzie można określić dokładniej, w jakim zakresie dostosowawczym uczelnia będzie musiała wprowadzić zmiany.