UZASADNIENIE

Opracowanie projektu nowej ustawy o ochronie danych osobowych wynika z konieczności zapewnienia stosowania 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".

Rozporządzenie będzie obowiązywało w polskim porządku prawnym bezpośrednio i będzie miało zastosowanie od dnia 25 maja 2018 r. i od tego dnia polskie przepisy muszą zapewniać skuteczne stosowanie przepisów Rozporządzenia, nie powielając jego rozwiązań ani nie będąc z nim sprzecznymi. Zakres kompetencji państw członkowskich wdrażania przepisów Rozporządzenia wyznacza co do zasady samo rozporządzenie (zob. szerzej P. Kozik, „Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego" EPS 5/2017 s. 18-22).

Przepisy obowiązującej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r, poz. 922), zwanej dalej „obowiązującą Ustawą", z jednej strony zawierają regulacje analogiczne do regulacji Rozporządzenia, np. w zakresie definicji danych osobowych, z drugiej zawierają regulacje odmienne niż te, które przewiduje Rozporządzenie, choćby w zakresie definicji zgody osoby, której dane dotyczą. Obowiązująca Ustawa zawiera też regulacje, których nie przewiduje Rozporządzenie, np. w zakresie rejestracji zbiorów danych, ale także brak w obowiązującej ustawie przepisów dotyczących choćby certyfikacji.

W świetle powyższego konieczne stało się opracowanie zupełnie nowej regulacji w zakresie ochrony danych osobowych, która odpowiadałaby przepisom i standardom ochrony danych osobowych przyjętym na poziomie UE. Przepisy projektowanej ustawy ustanawiają nowy organ właściwy w sprawie ochrony danych osobowych będzie nim Prezes Urzędu Ochrony Danych Osobowych.

W **Rozdziale 1** wskazano zakres podmiotowy i przedmiotowy regulacji. Zgodnie z art. 1, ustawa będzie miała zastosowanie do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Wobec powyższego przepisy ustawy nie znajdą zastosowania do ochrony innych podmiotów w związku z przetwarzaniem ich danych

osobowych. Powyższe odpowiada zakresowi podmiotowemu zastosowania Rozporządzenia i jest zgodne z motywem 14 preambuły do Rozporządzenia, który stanowi, że „Ochrona zapewniana niniejszym Rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych. Niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych, dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej.” Jednocześnie nie zdecydowano się skorzystać z możliwości przyjęcia przepisów o przetwarzaniu danych osobowych osób zmarłych. W tym zakresie instrumentem ochrony będą przepisy o ochronie dóbr osobistych przewidziane w kodeksie cywilnym (np. w ramach kultu pamięci osoby zmarłej).

W projekcie ustawy przyjęto, że przedmiotowy zakres jej zastosowania będzie odpowiadał zakresowi zastosowania Rozporządzenia, co oznacza, że będzie miała zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących lub mających stanowić część zbioru danych.

Stosowanie nowej ustawy – zgodnie z treścią Rozporządzenia - będzie wyłączone w odniesieniu do przetwarzania danych osobowych:

1) w ramach działalności nieobjętej zakresem prawa Unii;

2) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 Traktatu o funkcjonowaniu Unii Europejskiej;

3) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;

4) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Projektodawca, przyjął w projekcie nowej ustawy dokładnie taki sam zakres przedmiotowy, jak w przypadku Rozporządzenia, uznając, iż jest on adekwatnie szeroki, podobnie jak w obowiązującej Ustawie. Jednocześnie przyjął, że wyjątki od stosowania nowej ustawy stanowią katalog zamknięty i muszą być stosowane zawężająco. Stąd w trakcie prac nad projektem nowej ustawy rozważano, jakie sprawy będą mogły być wyłączone z zakresu jej stosowania jako działalność nieobjęta prawem UE. Ostatecznie przyjęto, że wyłączenie to ma bardzo wąski charakter, gdyż działania podejmowane przez państwa członkowskie, w

których mamy do czynienia z przetwarzaniem danych osobowych, będą podlegały regułom wynikającym z Rozporządzenia, ze względu na konieczność zapewnienie tym danym ochrony na takich samych warunkach we wszystkich państwach członkowskich. Projektodawca nie zdecydował się również na poszerzenie zakresu zastosowania Rozporządzenia na obszary objęte kompetencjami koordynacyjnymi, przewidzianymi w art. 6 Traktatu o Funkcjonowaniu Unii Europejskiej. Wejście w życie Traktatu z Lizbony wprowadziło bowiem w tym zakresie znaczącą zmianę. Traktat zniósł strukturę filarową w UE oraz wprowadził ogólną podstawę prawną do przyjęcia jednolitych ram prawnych ochrony danych osobowych w art. 16 TFUE, obejmując nimi były I oraz III filar UE. Obszary te objęte są więc działalnością unifikacyjną Unii Europejskiej w zakresie objętym Rozporządzeniem.

Jednocześnie biorąc pod uwagę potrzebę jednolitego stosowania Rozporządzenia nie zdecydowano się na poziomie projektowanej ustawy zdefiniować pojęć wyznaczających zakres wyłączeń stosowania Rozporządzenia. Projektodawca – mimo podobnych działań podejmowanych przez inne państwa członkowskie, nie zdecydował się również na ograniczenie zastosowania przepisów o ochronie danych osobowych wyłącznie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Polsce uznając, że stanowiłoby to ograniczenie art. 3 Rozporządzenia. Szczegółowy zakres przedmiotowy projektowanej ustawy określa art. 1 ust. 2 projektu.

Uwzględniając, że ustawa służy zapewnieniu skutecznego stosowania w polskiej przestrzeni prawnej Rozporządzenia, jego treść wyznacza zakres terytorialny jej stosowania. Tym samym ustawę stosuje się 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.

Nowa ustawa - zgodnie z przepisami Rozporządzenia - będzie miała zastosowanie także do przetwarzania danych osób, przebywających w Unii przez administratora lub podmiot przetwarzający niemający jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

Nowa ustawa będzie też stosowana do 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.

W przepisach ogólnych projektowanej ustawy, w art. 2, wyłączono stosowanie niektórych przepisów Rozporządzenia do:

- działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych,

- działalności literackiej,

- działalności artystycznej,

- wypowiedzi akademickiej.

Rozporządzenie posługuje się terminem wypowiedzi akademickiej, artystycznej lub literackiej. Projektodawca zdecydował się na wprowadzenie terminu działalności literackiej i artystycznej, termin „wypowiedź" stosując wyłącznie względem aktywności akademickiej. Rozwiązanie podyktowane jest tym, że w ocenie projektodawcy termin „działalność" w kontekście aktywności literackiej i artystycznej jest tożsamy z terminem wypowiedź. Każda działalność artystyczna i literacka podejmowana jest bowiem, celem osiągnięcia rezultatu jakim jest wypowiedź artystyczna i literacka twórcy wyrażona w określonej formie. Jednocześnie termin „wypowiedź artystyczna" oraz „wypowiedź literacka" jest obcy polskiemu prawodawstwu. Odmiennie należy jednak ocenić określenie „wypowiedzi akademickiej", gdyż w ramach aktywności akademickiej sama wypowiedź stanowi tylko jeden z elementów działań podejmowanych przez uczelnie wyższe, które prowadzą zakrojoną na szeroką skalę działalność organizatorską, która nie zawsze może jednak zostać zakwalifikowana jako „wypowiedź akademicka".

Możliwość dokonania takich wyłączeń wynika z przepisu art. 85 Rozporządzenia. Zgodnie z tym przepisem państwa członkowskie przyjmują przepisy, pozwalające pogodzić prawo do ochrony danych osobowych na mocy Rozporządzenia z wolnością wypowiedzi i informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej.

Dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej państwa członkowskie określają odstępstwa lub wyjątki od rozdziału II (Zasady), rozdziału III (Prawa osoby, której dane dotyczą), rozdziału IV (Administrator i podmiot przetwarzający), rozdziału V (Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych), rozdziału VI (Niezależne organy

nadzorcze), rozdziału VII (Współpraca i spójność) oraz rozdziału IX (Szczególne sytuacje związane z przetwarzaniem danych), jeżeli są one niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji. Należy zwrócić uwagę, iż art. 85 Rozporządzenia stanowi samodzielną podstawę wyżej wymienionych wyłączeń bez potrzeby odwoływania się do treści art. 23 Rozporządzenia.

Proponowane brzmienie art. 2 projektu nowej ustawy o ochronie danych osobowych wskazuje relacje pomiędzy ochroną danych osobowych a działalnością dziennikarską, artystyczną, literacką i wypowiedzią akademicką. Przewidziane w nim wyłączenia stosowania przepisów Rozporządzenia uznano za niezbędne dla pogodzenia prawa do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji. Wyłączenia te mają pierwszeństwo, o ile korzystanie z nich nie narusza istotnie praw lub wolności podmiotu danych, np. poprzez wykorzystanie tych danych faktycznie w innym celu niż twórczość dziennikarska, artystyczna lub literacka (np. w celu zniesławienia).

W przypadku wszystkich ww. rodzajów wypowiedzi akademickiej wyłączono stosowanie art. 13,15 ust. 3 i 4, art. 18, art. 27, art. 28 ust. 2-10 oraz art. 30 Rozporządzenia.

Wyłączono zatem następujące obowiązki administratora lub podmiotu przetwarzającego:

- informowanie osoby, której dane dotyczą o danych pozyskanych od tej osoby (art. 13),

- dostarczania osobie, której dane dotyczą kopii danych (art. 15 ust. 3 oraz ust. 4),

- ograniczenia przetwarzania na wniosek osoby, której dane dotyczą (art. 18),

- wyznaczania swojego przedstawiciela w UE w przypadku, o którym mowa w art. 3 ust. 2 Rozporządzenia (art. 27),

- powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu na podstawie umowy lub innego instrumentu prawnego (art. 28),

- prowadzenia rejestru czynności przetwarzania danych osobowych (art. 30).

Dodatkowo do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych, działalności literackiej oraz działalności artystycznej, nie będzie się stosowało następujących przepisów Rozporządzenia:

- art. 5 – zasady przetwarzania danych osobowych,

- art. 6 – przesłanki legalności przetwarzania danych osobowych,

- art. 7 – warunki wyrażania zgody przez osobę, której dane dotyczą,

- art. 8 - warunki wyrażania zgody przez dziecko w przypadku usług społeczeństwa informacyjnego,

- art. 9 – przetwarzanie szczególnych kategorii danych,

- art. 11 – przetwarzanie danych osobowych osoby nie wymagającej identyfikacji,

- art. 14 – obowiązek podawania informacji w przypadku pozyskiwania danych nie od osoby, której dane dotyczą,

- art. 15 ust. 1 i 2 – prawo dostępu przysługujące osobie, której dane dotyczą,

- art. 16 – prawo do sprostowania danych,

- art. 19 – obowiązek powiadomienia odbiorcy danych o sprostowaniu, lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,

- art. 20 – prawo do przenoszenia danych,

- art. 21 – prawo do sprzeciwu,

- art. 22 – zautomatyzowane podejmowanie decyzji w indywidualnych sprawach, w tym profilowanie.

W ocenie projektodawcy ww. wyłączenia „realizują" motyw 153 Rozporządzenia zgodnie z którym „Prawo państw członkowskich powinno godzić przepisy, regulujące wolność wypowiedzi i informacji, w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia. Przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, przewidzianymi w art. 11 Karty praw podstawowych. Powinno mieć to zastosowanie w szczególności do przetwarzania danych osobowych w dziedzinie audiowizualnej oraz w archiwach i bibliotekach prasowych. Państwa członkowskie powinny więc przyjąć akty prawne określające odstępstwa i wyjątki niezbędne do zapewnienia równowagi między tymi prawami podstawowymi. Państwa członkowskie powinny przyjąć takie odstępstwa i wyjątki w odniesieniu do zasad ogólnych, praw przysługujących osobie, której dane dotyczą, administratora i podmiotu przetwarzającego, przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, niezależnych organów

nadzorczych, współpracy i spójności oraz szczególnych sytuacji przetwarzania danych. Jeżeli odstępstwa i wyjątki różnią się zależnie od państwa członkowskiego, zastosowanie powinno mieć prawo państwa członkowskiego, któremu podlega administrator. Aby uwzględnić, jak ważna dla każdego demokratycznego społeczeństwa jest wolność wypowiedzi, pojęcia dotyczące tej wolności, takie jak dziennikarstwo, należy interpretować szeroko.

Art. 3 projektu wdraża do polskiego porządku prawnego regulację art. 8 ust. 1 *in fine* Rozporządzenia. Zgodnie z treścią art. 8 ust. 1 Rozporządzenia:

„Jeżeli zastosowanie ma art. 6 ust. 1 lit. a, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat.”.

Art. 8 Rozporządzenia wyraża bezpośrednio skuteczną normę z wąsko określonym obszarem kompetencji państw członkowskich. Państwa członkowskie mają swobodę regulacyjną w określeniu granicy wieku dziecka, jeżeli zastosowanie ma art. 6 ust. 1 lit. a Rozporządzenia w przypadku usług społeczeństwa informacyjnego, oferowanych bezpośrednio dziecku. Państwa członkowskie mają w tym zakresie swobodę wyboru granicy wieku (tj. granicy powyżej, której dziecko może samodzielnie wyrazić zgodę), ale wyłącznie w odniesieniu do osób, które ukończyły 13 lat. Należy podkreślić, iż jest to wyłącznie możliwość po stronie państw członkowskich, bez konieczności skorzystania z kompetencji regulacyjnej.

Co istotne, wskazana podstawa kompetencyjna dotyczy wyłącznie określenia granicy wieku dla skutecznego wyrażenia zgody przez dziecko i tylko w przypadku usług społeczeństwa informacyjnego, oferowanych bezpośrednio dziecku. Oznacza to w szczególności, iż art. 8 ust. 1 *in fine* Rozporządzenia nie przyznaje państwom członkowskim kompetencji do:

a) określenia ogólnej granicy wieku dla możliwości przetwarzania danych osobowych dziecka (niezależnie od podstawy legalizującej przetwarzanie danych osobowych);

b) modyfikacji zasad związania umową (art. 6 ust. 1 lit. b Rozporządzenia np. umowa o świadczenie usług drogą elektroniczną) jako podstawą przetwarzania danych (regulują to odrębne przepisy prawa umów państw członkowskich zgodnie z art. 8 ust. 3 Rozporządzenia);

c) określania mechanizmu wyrażania lub aprobowania zgody dziecka (tj. w jakiej sytuacji przedstawiciel ustawowy może zgodę wyrazić samodzielnie, a w jakiej wyłącznie potwierdza czynność dziecka);

d) regulacji sposobów weryfikacji tożsamości udzielających zgodę;

d) określania tego kto i w jakim trybie może zgodę wycofać;

e) regulacji problemu zgody – jako podstawy legalizującej przetwarzanie danych osobowych zgodnie - poza obszarem usług społeczeństwa informacyjnego (usług świadczonych drogą elektroniczną);

f) regulacji problemu zgody osoby ubezwłasnowolnionej.

Dodatkowo należy zwrócić uwagę, iż o ile art. 8 ust. 1 Rozporządzenia przesądza powyżej jakiej granicy wieku dziecko może samodzielnie udzielić zgody na przetwarzanie danych osobowych w ramach usług społeczeństwa informacyjnego, o tyle nie przesądza granicy wieku poniżej, której dziecko zgody w ogóle wyrazić nie może. Poniżej określonej granicy wieku (w przedziale 13-16 lat) w obrębie art. 8 ust. 1 Rozporządzenia, zgodę, o której mowa w art. 6 ust. 1 lit. a Rozporządzenia może wyrazić zarówno samodzielnie przedstawiciel ustawowy, jak i dziecko, jednak w tym drugim przypadku zgoda jest skuteczna po potwierdzeniu jej przez rodzica lub opiekuna prawnego.

W kontekście powyższego (niezależnie od oceny przedstawionej regulacji Rozporządzenia) należy wyraźnie podkreślić, iż przepisy Rozporządzenia (art. 8 ust. 1) nie przyznają państwom członkowskim kompetencji określenia granicy wieku, poniżej której dziecko w ogóle zgody - na przetwarzanie danych osobowych w zakresie usług społeczeństwa informacyjnego - wyrazić nie może. W tym zakresie w praktyce należy odwołać się przede wszystkich do ogólnych kryteriów skuteczności zgody wskazanych w art. 4 pkt 11, zgodnie z którym: „zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w formie oświadczenia lub wyraźnego działania, potwierdzającego, przyzwolenie na przetwarzanie dotyczących jej danych osobowych.

Projekt realizując kompetencję wskazaną w art. 8 ust. 1 *in fine* Rozporządzenia, obniża granicę wieku określoną w tym przepisie. Oznacza to, że zgodnie z projektem samodzielnie zgodę na przetwarzanie danych osobowych w przypadku usług społeczeństwa

informacyjnego oferowanych bezpośrednio dziecku (np. zgodę na przetwarzanie danych osobowych w celu marketingu bezpośredniego administratora danych) będzie mogła wyrazić osoba, która ukończyła lat 13. Jednocześnie w celu zapewnienia pełnej efektywności regulacji art. 8 ust. 1 Rozporządzenia precyzuje, iż:

a) problem zgody dotyczy usług świadczonych drogą elektroniczną, oraz

b) wyrazić lub zaaprobować zgodę (wyrażoną przez dziecko, które nie ukończyło lat 13) może przedstawiciel ustawowy.

Ad. a)

Art. 8 ust. 1 Rozporządzenia posługuje się pojęciem usług społeczeństwa informacyjnego. Zgodnie natomiast z art. 4 pkt 25 Rozporządzenia, „usługa społeczeństwa informacyjnego" oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535. Biorąc pod uwagę treść art. 1 ust. 1 lit. b) Dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1), pojęcie „usługi społeczeństwa informacyjnego" należy traktować jako tożsame pojęciu: „usługi świadczonej drogą elektroniczną" zgodnie z treścią ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. W związku z tym w celu uniknięcia wątpliwości co do zakresu zastosowania art. 3 projektu, w tym zachowania systemowej zgodności, projekt w art. 3 posługuje się określeniem „usługi świadczonej drogą elektroniczną".

Ad. b)

Identyfikacja osoby uprawnionej do wyrażenia uprzedniej zgody (w oparciu o projektowany art. 3 ustawy) albo do potwierdzenia zgody wyrażonej przez osobę, która nie ukończyła lat 13 powinno następować przy uwzględnieniu treści przepisów ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny, dalej „k.c.", oraz ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy. W związku z tym projekt posługuje się ogólnym pojęciem przedstawiciela ustawowego.

Projektodawca zdecydował się skorzystać z kompetencji przyznanej mu na mocy art. 8 ust. 1 *in fine* Rozporządzenia. Można założyć, iż wskazana podstawa kompetencyjna ma na celu dostosowanie przepisów Rozporządzenia do ogólnych reguł skutecznego składania oświadczeń woli przez dzieci w systemach prawnych państw członkowskich, w tym w zakresie regulacji prawa prywatnego. Na marginesie należy zwrócić uwagę, iż przepisy o ochronie danych osobowych wprost odwołują się do prawa prywatnego w kontekście zgody

na przetwarzanie danych osobowych. Motyw 42 Rozporządzenia, wskazuje, iż zgodnie z dyrektywą Rady 93/13/EWG (tj. w sprawie nieuczciwych warunków w umowach konsumenckich) oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem oraz nie powinno zawierać nieuczciwych warunków.

Należy zwrócić uwagę, iż w polskim systemie prawa cywilnego granicę wieku, kiedy małoletni może składać skuteczne (niekonieczne samodzielnie) oświadczenia woli, wyznacza ukończenie 13 lat. Zgodnie z art. 15 k.c. ograniczoną zdolność do czynności prawnych mają małoletni, którzy ukończyli lat trzynaście oraz osoby ubezwłasnowolnione częściowo. Ograniczona zdolność do czynności prawnych oznacza, iż małoletni może składać oświadczenia woli, z tym, że pewnych sytuacjach do ich skuteczności wymagana jest zgoda przedstawiciela ustawowego.

Przyjmując regulację kodeksu cywilnego jako „wzorzec regulacyjny" i możliwy punkt odniesienia przy ocenie adekwatnego wieku podejmowania świadomych decyzji przez małoletnich, należy wskazać, iż wyrażenie zgody na przetwarzanie danych osobowych stanowi jednocześnie oświadczenie woli w rozumieniu k.c.

W piśmiennictwie zauważono, iż w świetle regulacji k.c. zgoda na przetwarzanie danych osobowych nie podlega ograniczeniom wskazanym w art. 17 w zw. z art. 19 k.c. (nie jest to ani czynność prawna rozporządzająca ani zobowiązująca). Dlatego w świetle k.c. skuteczną zgodę na przetwarzanie danych osobowych może samodzielnie wyrazić osoba, która ma co najmniej ograniczoną zdolność do czynności prawnych (przede wszystkim ukończyła lat 13 * – zob. szerzej M. Gumularz, „Charakter prawny oświadczenia w zakresie zgody na przetwarzanie danych", ABI Expert z 2017, nr 2). Zgoda osoby, która ukończyła 13 lat (i nie została ubezwłasnowolniona całkowicie) będzie legalizować ingerencję w dobro osobiste – dane osobowe – na gruncie art. 24 k.c.

W związku z powyższym z systemowego punktu widzenia istotne jest, aby ocena tego samego zachowania na gruncie różnych reżimów (ochrona danych osobowych oraz prawo cywilne) nie prowadziła do odmiennych wniosków co do skuteczności. Uzasadnia to przyjęcie granicy wieku 13 lat.

W **Rozdziale 2** projektowanej ustawy uregulowano tryb notyfikacji inspektorów ochrony danych osobowych, zwanych dalej „inspektorami" oraz podmioty obowiązane w polskim porządku prawnym do wyznaczenia inspektora ochrony danych osobowych.

Rozporządzenie reguluje kwestię inspektorów w przepisach art. 37-39. Przypadki obligatoryjnego wyznaczenia inspektorów określa art. 37 Rozporządzenia. Zgodnie z tym przepisem administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze, gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

W innych niż ww. przypadkach wyznaczenie inspektora jest dobrowolne. Projektodawca nie zdecydował się rozszerzyć przedmiotowo sytuacji obligatoryjnego wyznaczania inspektora, traktując katalog wymieniony w art. 37 ust. 1 Rozporządzenia jako zapewniający dostateczną ochronę podmiotów danych a jednocześnie uwzględniający także koszty powołania inspektora.

Rozporządzenie nie definiuje terminu „organu lub podmiotu publicznego". Grupa Robocza art. 29, jako unijne forum współpracy organów ochrony danych osobowych Państw Członkowskich UE, wskazała w swoich wytycznych, dotyczących inspektorów ochrony danych (WP243), „że takie pojęcie powinno zostać określone na poziomie przepisów krajowych. Do podmiotów takich najczęściej zalicza się organy władzy krajowej, organy regionalne i lokalne, ale również – na mocy właściwego prawa krajowego - szereg innych podmiotów prawa publicznego". Uwzględniając powyższe oraz treść Rozporządzenia, wskazującego na obowiązek wyznaczenia inspektorów, ciążący na „organach lub podmiotach publicznych", projektodawca zdecydował się wprowadzić do projektu szerokie rozumienie takich podmiotów publicznych. Przepis art. 4 projektu w celu zapewnienia stosowania art. 37 ust. 1 lit. a Rozporządzenia precyzuje, iż organami i podmiotami publicznymi obowiązanymi do wyznaczenia inspektora są organy publiczne wskazane w art. 5 par. 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, zwanego dalej „Kodeksem", oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Na gruncie polskiego porządku prawnego odesłanie w zakresie pojęć „organ

publiczny" i „podmiot publiczny", do dwóch ww. ustaw, jako regulacji o podstawowym znaczeniu dla interpretacji ww. pojęć, wydaje się rozwiązaniem najbardziej racjonalnym i systemowo spójnym.

Kwalifikacje, jakie powinien posiadać inspektor określono bezpośrednio w Rozporządzeniu. Z jego przepisów wynika, iż inspektor powinien dysponować wiedzą fachową na temat prawa oraz odbyć praktyki w dziedzinie ochrony danych, a także posiadać umiejętność wypełniania zadań, o których mowa w art. 39 Rozporządzenia. Projektodawca nie zdecydował się na dookreślenie kwalifikacji, jakie powinien spełniać inspektor, wychodząc z założenia, że każda próba doprecyzowania tych przesłanek - np. w zakresie długości praktyk - mogłaby narazić go na zarzut nakładania ograniczeń, nie występujących w innych Państwach Członkowskich UE, a tym samym barierę w swobodzie świadczenia usług. Co do umiejętności wypełniania zadań, to należy podkreślić, iż odpowiedzialność za wybór inspektora, a tym samym za umiejętność wykonywania zadań, ponosi administrator. To w jego interesie leży taki wybór inspektora, który da mu rękojmię umiejętnego wykonywania przez niego zadań. Grupa Robocza art. 29 wskazała w swoich wytycznych nr WP 243, dotyczących inspektorów ochrony danych, że wymagany rozporządzeniem 2016/679 „poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych, przetwarzanych w ramach jednostki. Dla przykładu, w przypadku wyjątkowo skomplikowanych procesów przetwarzania danych osobowych lub w przypadku przetwarzania dużej ilości danych szczególnych kategorii, inspektor może potrzebować wyższego poziomu wiedzy i wsparcia. Ponadto inaczej sytuacja przedstawiać się będzie w przypadku podmiotów regularnie przekazujących dane do państw trzecich niż w przypadku, gdy przekazywanie takie ma charakter okazjonalny. W związku z tym wybór inspektora powinien być dokonany z zachowaniem należytej staranności i brać pod uwagę charakter przetwarzania danych w ramach podmiotu". Z kolei wypowiadając się w przedmiocie kryterium kwalifikacji zawodowych, Grupa wskazała, że „istotne jest, by inspektor posiadał odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość RODO. Propagowanie odpowiednich i regularnych szkoleń dla inspektorów przez organy nadzorcze również może być przydatne. Przydatna jest również wiedza na temat danego sektora i podmiotu administratora. Inspektor powinien również posiadać odpowiednią wiedzę na temat operacji przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych. W przypadku organów i podmiotów publicznych Inspektor powinien również posiadać wiedzę w zakresie procedur administracyjnych i funkcjonowania jednostki". Powyższe stanowiska wskazują więc

skuteczny kierunek wykładni przepisów rozporządzenia 2016/679 i są praktycznym drogowskazem dla inspektorów (dzisiejszych Administratorów Bezpieczeństwa Informacji, zwanych dalej „ABI"). Jednocześnie należy wskazać, że w dzisiejszym porządku prawnym ustawodawca także nie wypowiada się w przedmiocie kwalifikacji zawodowych koniecznych do pełnienia funkcji ABI. Przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wskazują bowiem, że funkcję taką może pełnić osoba, posiadająca odpowiednią wiedzę w zakresie ochrony danych osobowych. Weryfikację takiego kryterium podejmuje więc w każdym przypadku przedsiębiorca zatrudniający ABI oraz Generalny Inspektor Ochrony Danych Osobowych na etapie przeprowadzanych postępowań kontrolnych.

Co ważne, projekt nowej ustawy przewiduje, że inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. W tym miejscu należy zwrócić także uwagę, iż art. 37 Rozporządzenia nie przyznaje państwom członkowskim kompetencji do określenia w ilu maksymalnie podmiotach dana osoba może pełnić funkcję inspektora.

Przepisy Rozporządzenia przewidują także, że administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora i zawiadamiają o nich organ nadzorczy. Na tej podstawie prowadzona jest przez Prezesa Urzędu wewnętrzna ewidencja – przepisy Rozporządzenia nie wprowadzają obowiązku prowadzenia jawnego rejestru inspektorów. Natomiast obowiązek publikacji danych kontaktowych inspektora spoczywa zgodnie z art. 37 ust. 7 Rozporządzenia na administratorze oraz podmiocie przetwarzającym. Realizacji tego właśnie przepisu służy art. 5 projektu, regulujący sposób i tryb zawiadamiania o wyznaczeniu inspektora oraz prowadzenie ewidencji zawiadomień. Przewidując dużą liczbę zawiadomień, kierowanych w przyszłości do organu, przyjęto rozwiązanie, zgodnie z którym zawiadomienia należy przesyłać drogą elektroniczną. Co istotne, w zawiadomieniu należy wskazać adres poczty elektronicznej lub numer telefonu osoby wyznaczonej do pełnienia roli inspektora. Art. 5 projektu w sposób zamierzony nie przesądza, czy może to być adres e-mail ogólny (np. IOD@...) czy przypisany do konkretnej osoby (np. jan.kowalski@...). W praktyce należy dopuścić obie możliwości.

Na gruncie obowiązującej Ustawy podmiotem, który pełni podobną funkcję jak inspektor jest ABI. Powołanie ABI jest dobrowolne. Zadania ABI-ego określa art. 36a obowiązującej Ustawy.

Co istotne, przepisy Rozporządzenia nie przewidują możliwości wprowadzenia przez państwa członkowskie szczególnych regulacji w zakresie statusu i zadań inspektora.

Rozdział 3 projektu reguluje zasady certyfikacji i akredytacji oraz tryb postępowania w tych sprawach.

Zgodnie z art. 42 ust. 1 Rozporządzenia Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, mających świadczyć o zgodności z Rozporządzeniem operacji przetwarzania, prowadzonych przez administratorów i podmioty przetwarzające.

W projekcie przewidziano, że certyfikacji dokonywał będzie wyłącznie Prezes Urzędu Ochrony Danych Osobowych, tym samym w projekcie nie było konieczne uregulowanie procedury akredytacji podmiotów certyfikujących. Zgodnie z art. 42 ust. 5 Rozporządzenia certyfikacji dokonują podmioty certyfikujące, o których mowa w art. 43 Rozporządzenia, lub dokonuje jej właściwy organ nadzorczy. Ustawodawca unijny przyznał więc państwom członkowskim swobodę w wyborze podmiotu który podejmował będzie działania certyfikacyjne. Zdecydowano o przyznaniu uprawnień do podejmowania działań certyfikacyjnych Prezesowi Urzędu Ochrony Danych Osobowych.

Jednocześnie należy wskazać, że w ocenie projektodawcy jednostka odpowiadająca za certyfikację wewnątrz struktury organizacyjnej Urzędu Ochrony Danych Osobowych nie powinna odpowiadać za prowadzenie postępowań w sprawie naruszenia przepisów o ochronie danych, w tym przeprowadzanie czynności kontrolnych. Ich powiązanie byłoby bowiem czynnikiem korupcjogennym lub generującym ryzyka braku obiektywizmu w przypadku kontroli. Podejmowaniu czynności certyfikacyjnych towarzyszyć powinna pełna bezstronność. Struktura organizacyjna organu nadzorczego powinna przyznawać temu pionowi pełną gwarancję bezstronności.

Przyznanie Prezesowi Urzędu wyłącznych kompetencji do podejmowania czynności certyfikacyjnych stanowi uzasadnienie do zwiększenia liczby zastępców organu. Bez wątpienia rekomendowanym rozwiązaniem byłoby przyznanie jednemu z nich kompetencji do wspierania Prezesa Urzędu w kierowaniu jednostką odpowiadającą za certyfikację w tym w zapewnieniu jej pełnej niezależności względem pozostałych jednostek jego struktury organizacyjnej.

Certyfikacji dokonuje się na wniosek administratora lub podmiotu przetwarzającego. Certyfikacji dokonuje się na podstawie kryteriów określonych przez Prezesa Urzędu i udostępnionych w BIP na jego stronie podmiotowej.

Postępowanie w sprawie udzielenia certyfikacji może zakończyć się czynnością materialno-techniczną jaką jest zawiadomienie wnioskodawcy o udzieleniu lub odmowie udzielenia certyfikacji. Natomiast odmowa udzielenia certyfikacja wiązała się będzie z obowiązkiem wydania decyzji administracyjnej. Wydając decyzję o odmowie udzielenia certyfikacji Prezes Urzędu obowiązany będzie wskazać kryteria, których nie spełnienie było powodem odmowy.

W przepisie art. 15 wskazano sytuacje kiedy cofa się certyfikację. Cofnięcie certyfikacji również następowało będzie w drodze decyzji administracyjnej. Certyfikacji udziela się na maksymalny okres 3 lat co wynika wprost z art. 42 ust. 7 Rozporządzenia. Przez cały ten okres administrator lub podmiot przetwarzający są obowiązani spełniać kryteria certyfikacji. W celu zapewnienia skutecznych narzędzi sprawdzania, czy kryteria certyfikacji są spełniane, przewidziano uprawnienie dla Prezesa Urzędu do przeprowadzania czynności sprawdzających. Zakres uprawnień przysługujących w ramach prowadzenia czynności sprawdzających określa art. 14 projektu. Dokumentem potwierdzającym certyfikację jest certyfikat.

Przepisy art. 17-19 projektu dotyczą monitorowania przestrzegania zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 Rozporządzenia. Przepis ten stanowi m.in., iż państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia - z uwzględnieniem specyfiki różnych sektorów, dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz MŚP (Małych i Średnich Przedsiębiorstw). Zrzeszenia i inne podmioty, reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie niniejszego rozporządzenia. Projekt nowej ustawy przewiduje, iż monitorowaniem przestrzegania zatwierdzonego kodeksu postępowania będą zajmowały się podmioty akredytowane przez Prezesa Urzędu. Prezes Urzędu będzie udostępniał wykaz podmiotów akredytowanych w Biuletynie Informacji Publicznej.

Rozdział 4 zawiera kluczową regulację ustrojową – przepisy, dotyczące Prezesa Urzędu Ochrony Danych Osobowych. Przepis art. 8 obowiązującej Ustawy stanowi, że organem do spraw ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych. Przepisy projektowanej ustawy ustanawiają nowy organ właściwy w sprawie ochrony danych osobowych, będzie nim Prezes Urzędu Ochrony Danych Osobowych. Zgodnie z motywem 117 Rozporządzenia „zasadniczym elementem ochrony osób fizycznych

w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, uprawnionych do wypełniania zadań i wykonywania uprawnień w sposób całkowicie niezależny". Każde z Państw Członkowskich w świetle przyznanej im zasady autonomii instytucjonalnej oraz proceduralnej może ustanowić więc niezależny aparat państwowy, nadzorujący przestrzeganie przepisów Rozporządzenia. Ponieważ uchylona zostaje podstawa prawna działania Generalnego Inspektora Ochrony Danych Osobowych – co jest konieczne celem wydania aktu zapewniającego skuteczne stosowanie Rozporządzenia a obecna Ustawa implementuje uchylaną dyrektywę, nowy organ nadzorczy z prawnego punktu widzenia jest nowym organem państwowym, będącym następcą prawnym Generalnego Inspektora.

Do nadania organowi nadzorczemu nazwy Prezesa Urzędu Ochrony Danych Osobowych skłoniła Projektodawcę treść przepisów Rozporządzenia , a decyzja w tym zakresie ma wyłącznie wymiar porządkujący. Po pierwsze, Rozporządzenie wprowadza funkcję „inspektora ochrony danych" jako osoby fizycznej wyznaczanej przez administratora bądź podmiot przetwarzający wewnątrz ich struktury organizacyjnej i obowiązanej do szeroko rozumianego monitorowania przestrzegania Rozporządzenia. Jednocześnie brak jest jednak jakiegokolwiek związku ustrojowego pomiędzy takimi osobami a przyszłym organem nadzorczym, odpowiadającym za egzekwowanie w Polsce przestrzegania przepisów Rozporządzenia. Przyjęcie obecnej nazwy organu wprowadzałoby w tym zakresie w błąd, w tym co do ich pozycji ustrojowej. Zgodnie bowiem z art. 38 ust. 3 Rozporządzenia inspektorzy ochrony danych muszą być niezależni. Po drugie utrzymanie obecnej nazwy - Generalny Inspektor Ochrony Danych Osobowych powodowałoby niejako konieczność nazwania inspektorami pracowników biura, którzy w imieniu organu przeprowadzają postępowanie kontrolne. Skoro bowiem mamy Generalnego Inspektora, muszą funkcjonować w jego strukturze organizacyjnej inni inspektorzy, względem których jest on inspektorem generalnym (tak jak ma to miejsce na kanwie obowiązujących przepisów). Powyższe przesądziłoby z kolei, że w systemie ochrony danych osobowych mielibyśmy dwie kategorie inspektorów – pracowników organu nadzorczego oraz osoby mające zupełnie inny status powoływane wewnątrz struktury organizacyjnej administratorów i podmiotów przetwarzających, co jest w ocenie projektodawcy niedopuszczalne. Uwzględniając powyższe, odstąpiono również od nazywania pracowników organu nadzorczego przeprowadzających w jego imieniu czynności kontrolne inspektorami, na rzecz nazwania ich kontrolującymi. Projektodawca nadając organowi nazwę Prezesa Urzędu Ochrony Danych Osobowych dokonał wyczerpującej analizy nazewnictwa wykorzystywanego w Polsce względem innych organów państwowych. Uwagę należy w tym zakresie zwrócić chociażby

na Państwową Inspekcję Pracy i działających w jej ramach inspektorów pracy oraz społecznych inspektorów pracy. Po pierwsze bowiem, podmioty takie działają na zupełnie innej podstawie prawnej. O ile podstawą prawną działań podejmowanych przez inspektorów pracy jest ustawa z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy, o tyle podstawą działań podejmowanych przez społecznych inspektorów pracy jest ustawa z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy. Po drugie, z uwagi na zakres zadań prowadzonych przez społecznych inspektorów pracy przepisy nie podkreślają ich niezależności, jak ma to miejsce w Rozporządzeniu. Wręcz przeciwnie, zgodnie z art. 18 ustawy o społecznej inspekcji pracy, Państwowa Inspekcja Pracy udziela pomocy społecznej inspekcji pracy w realizacji jej zadań, w szczególności przez poradnictwo prawne, specjalistyczną prasę oraz szkolenie. Inspektorzy pracy Państwowej Inspekcji Pracy przeprowadzają kontrole wykonania zaleceń i uwag społecznych inspektorów pracy. Pomiędzy Państwową Inspekcją Pracy i społecznymi inspektorami pracy istnieje więc związek, którego brak jest w przypadku niezależnych względem organu nadzorczego inspektów ochrony danych. Wreszcie celem wyeliminowania wszelkich wątpliwości, społecznym inspektorom pracy nadano właśnie nazwę „społecznych inspektorów pracy", a nie „inspektorów pracy" by odróżnić ich od pracowników organu – czego nie można zrobić w przepisach zapewniających skuteczne stosowanie Rozporządzenia. Uwzględniając powyższe oraz doręczane Ministrowi Cyfryzacji różne postulaty, w tym od stowarzyszeń skupiających administratorów bezpieczeństwa informacji, najwłaściwszym jest użycie nazwy wykorzystywanej w Polsce najczęściej i najłatwiejszej do przyswojenia dla obywateli – Prezes Urzędu Ochrony Danych Osobowych. W trakcie prowadzonych prekonsultacji rozwiązanie takie zostało również poparte przez znaczną część izb gospodarczych oraz stowarzyszeń reprezentujących interesy administratorów bezpieczeństwa informacji.

Nowy organ ochrony danych osobowych będzie miał znacznie szerszy zakres uprawnień niż dzisiejszy GIODO. Będzie on nie tylko organem nadzorczym w rozumieniu Rozporządzenia ze znacznie szerszym zakresem uprawnień i obowiązków niż dzisiejszy GIODO, ale będzie również organem nadzorczym w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW. Projekt przepisów Rozporządzenia przewiduje również procedurę powołania Prezesa Urzędu. Ma być on powołany przez Sejm za zgodą Senatu na wniosek Prezesa Rady Ministrów. Rozporządzenie w art. 53 stanowi, iż

państwa członkowskie zapewniają, by każdy członek ich organów nadzorczych był powoływany w drodze przejrzystej procedury przez:

- ich parlament,
- ich rząd,
- ich głowę państwa, lub
- niezależny organ uprawniony do powoływania członków organu nadzorczego na podstawie prawa państwa członkowskiego.

Odnosząc się do ww. gwarancji niezależności nowego Prezesa Urzędu przyznawanych na etapie jego powołania uznano, że utrzymanie dotychczasowych rozwiązań w tym zakresie tj. tryb powoływania przez Sejm na wniosek Prezesa Rady Ministrów oraz przyznanie Prezesowi Urzędu immunitetu, analogicznie jak dotychczasowemu Generalnemu Inspektorowi Ochrony Danych Osobowych, będzie najlepszą gwarancją niezależności tego organu. Włączenie Prezesa Rady Ministrów w procedurę powołania Prezesa Urzędu uzasadnione jest pozycją ustrojową Prezesa Urzędu, który w trakcie swoich działań współpracuje zarówno w władzą ustawodawczą jak i wykonawczą, uczestnicząc w procedurze tworzenia prawa i sprawując nadzór nad przetwarzaniem danych osobowych we wszystkich obszarach działania państwa. W związku z powyższym, powołaniu na piastuna organu najlepszego kandydata towarzyszyć powinno pełne porozumienie pomiędzy zarówno władzą ustawodawczą jak i wykonawczą, przy przyznaniu jednak organowi wszelkich atrybutów jego niezależności – w tym jego podległość w zakresie wykonywanych zadań wyłącznie ustawie.

Regulację w zakresie warunków, jakie musi spełniać kandydat na Prezesa Urzędu określa art. 20 ust. 4 projektu. Projekt ustawy zawiera regulacje dotyczące zakazu członkostwa Prezesa Urzędu w partii politycznej, związku zawodowym, zakazu zajmowania innego stanowiska, z wyjątkiem stanowiska naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, wykonywania innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu oraz zakazu prowadzenia działalności publicznej niedającej się pogodzić z godnością jego urzędu. Do warunków których spełnienie stanowi wymóg objęcia stanowiska Prezesa Urzędu należy w szczególności pięcioletnie doświadczenie w wykonywaniu czynności bezpośrednio związanych z ochroną danych osobowych oraz posiadanie stopnia naukowego doktora. Spełnienie powyższych warunków w ocenie projektodawcy stanowi gwarancję objęcia stanowiska Prezesa Urzędu przez specjalistę posiadającego zarówno rozbudowaną teoretyczną jak i praktyczną wiedzę w obszarze ochrony danych osobowych. Projektodawca

wprowadzając wymóg posiadania stopnia doktora jako warunkujący pełnienie funkcji Prezesa Urzędu umocowuje godną pełnego poparcia i wykształconą od lat w Polsce praktykę powoływania na piastuna organu jakim jest Generalny Inspektor Ochrony Danych Osobowych osób posiadających taki stopień naukowy. Powyższe wpisuje się również w edukacyjną rolę organu nadzorczego jakim jest Generalny Inspektor Ochrony Danych Osobowych i jakim będzie Prezes Urzędu. Przy podejmowaniu decyzji w powyższym zakresie, projektodawca uwzględnił również kwalifikacje posiadane przez dotychczasowych piastunów organu jakim jest Generalny Inspektor Ochrony Danych Osobowych. Niemal każdy z nich posiadał stopień naukowy doktora nauk. Wskazane powyżej wymogi stanowią w ocenie projektodawcy dodatkową gwarancję niezależności organu poprzez podkreślenie jego apolitycznej i eksperckiej pozycji w ramach ustroju organów państwowych. W porównaniu z warunkami zawartymi w art. 8 ust. 3 obowiązującej Ustawy zrezygnowano z warunku stałego zamieszkiwania na terytorium Rzeczypospolitej Polskiej, jako nieuzasadnionego i trudnego do weryfikacji, zrezygnowano także z warunku dotyczącego wyróżniania się wysokim autorytetem moralnym jako trudno mierzalnego. W ocenie projektodawcy kryteria warunkujące możliwość pełnienia specjalistach kierowniczych funkcji państwowych powinny podlegać łatwej weryfikacji i mieć charakter formalny. Zmieniono również kryterium wykształcenia warunkującego możliwość ubiegania się o stanowisko Prezesa Urzędu. Piastun organu nie musi być bowiem prawnikiem, może być tytułem przykładu specjalistą w obszarze sektora IT bliskiego ochronie danych osobowych, posiadając jednak wiedzę z zakresu ochrony danych osobowych. Dodano wymóg korzystania z pełni praw publicznych oraz doprecyzowano wymóg niekaralności.

Projektowana ustawa przewiduje wprost, iż odwołanie Prezesa następuje w przypadku gdy Prezes zrzekł się stanowiska, stał się trwale niezdolny do pełnienia obowiązków na skutek choroby, został skazany prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego albo sprzeniewierzył się ślubowaniu. Nie przewidziano więc zmian w zakresie przesłanek odwołania. Szczególne wątpliwości w tym zakresie budzi art. 53 ust. 4 Rozporządzenia, w świetle którego *członek może zostać odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki niezbędne do pełnienia obowiązków*. Poważne uchybienie może stanowić zarówno rażące naruszenie prawa w związku z przewlekłością postępowania, jak i skazanie prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa. Uwzględniając jednak konieczność zapewnienia pełnej niezależności Prezesowi Urzędu, projektodawca odstąpił od wprowadzania do projektu przesłanki rażącego naruszenia prawa

jako podstawy do odwołania Prezesa Urzędu uznając, że jest nią skazanie prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa w tym przestępstwa skarbowego.

Gwarancją niezależności Prezesa Urzędu jest również przyznanie mu kompetencji do samodzielnego nadawania statutu. Novum przy regulacjach dotyczących tej jednostki jest nadawanie jej statutu przez Prezesa Urzędu, a nie jak jest w przypadku Generalnego Inspektoratu Ochrony Danych Osobowych przez Prezydenta RP. Organ sam decydował będzie więc o strukturze organizacyjnej Urzędu oraz zadaniach realizowanych przez jego zastępców oraz pracowników Urzędu. Nowością są również regulacje dotyczące obowiązku zachowania tajemnicy przez pracowników Urzędu. Powyższa regulacja ma za zadanie zapewnienie stosowania art. 54 ust. 2 Rozporządzenia.

Gwarancją niezależności organu jest również jego niezależność budżetowa.

Podobnie jak dzisiaj w przypadku GIODO, kadencja Prezesa Urzędu będzie trwała 4 lata i ta sama osoba nie będzie mogła być Prezesem Urzędu dłużej niż przez dwie kadencje.

W celu zapewnienia realizacji zadań nakładanych na nowy organ właściwy w sprawie ochrony danych osobowych oraz wzmocnienia jego pozycji przewidziano możliwość powołania do trzech zastępców Prezesa Urzędu. Rozwiązanie takie podyktowane jest bardzo szerokim zakresem zadań nałożonych na Prezesa Urzędu, które często wymagają innych kwalifikacji. Jako przykład można w tym zakresie podać wymóg prowadzenia współpracy międzynarodowej, podejmowania działań certyfikacyjnych, podejmowania działań edukacyjnych, prowadzenia postępowań w sprawach naruszenia przepisów o ochronie danych czy nadzoru nie tylko nad Rozporządzeniem ale również tzw. dyrektywą policyjną. Każde z tych działań może być przykładowo wspierane przez innego zastępcę Prezesa Urzędu. Ze względu na wykonywanie przez Prezesa Urzędu zadań organu nadzorczego w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, przewidziano w projekcie, iż jednego zastępcę Prezesa będzie powoływał Prezes Rady Ministrów na wniosek ministra właściwego do spraw wewnętrznych. Wniosek taki minister właściwy do spraw wewnętrznych będzie obowiązany przekazać celem zaopiniowania Ministrowi Sprawiedliwości, Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw finansów publicznych oraz Prokuratorowi Generalnemu.

Pozostali zastępcy powoływani będą na wniosek ministra właściwego do spraw informatyzacji. Uzasadnieniem do powoływania dwóch zastępców na wniosek właśnie ministra właściwego do spraw informatyzacji jest fakt, iż zgodnie z z art. 12a ust. 1 pkt 8 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2016 r., poz. 2260, z późn. zm.) do zakresu działania ministra właściwego do spraw informatyzacji należą sprawy kształtowania polityki państwa w zakresie ochrony danych osobowych .

Wreszcie nową instytucją powoływaną przez Prezesa Urzędu ma być Rada do Spraw Ochrony Danych Osobowych. W ocenie projektodawcy szeroki zakres zadań Prezesa Urzędu oraz potrzeba stałej grupy osób wspomagających Prezesa Urzędu w realizacji jego zadań uzasadniają powołanie przy Prezesie Urzędu organu opiniodawczo-doradczego. Skład Rady został tak zaprojektowany by mogły do niego wchodzić osoby reprezentujące różne podmioty, zarówno ze strony administracji publicznej, jak i spoza administracji (art. 34 ust. 7). Ideą jest by różne podmioty mogły wesprzeć swoją wiedzą Prezesa Urzędu. Zadania ww. Rady określa art. 34 ust. 2 projektu.

Przepis art. 35 projektu stanowi o sprawozdaniach składanych przez Prezesa Urzędu i służy zapewnieniu stosowania art. 59 Rozporządzenia.

Przepis art. 36 projektu nadaje Prezesowi Urzędu uprawnienie do opiniowania założeń i projektów aktów prawnych dotyczących danych osobowych. Z przepisu § 38 ust. 1 Regulaminu pracy Rady Ministrów wynika natomiast obowiązek kierowania przez organy wnioskujące projektów dokumentów rządowych do zaopiniowania przez organy administracji rządowej lub inne organy i instytucje państwowe, których zakresu działania dotyczy projekt. Celem przepisu art. 36 projektu jest zapewnienie stosowania art. 57 ust. 1 lit. c Rozporządzenia.

Regulacja zawarta w art. 37 projektu stanowi powielenie rozwiązań funkcjonujących i sprawdzających się na gruncie obowiązującej Ustawy zgodnie z którymi Prezes Urzędu może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Przepis art. 38 projektu dotyczy udostępniania przez Prezesa Urzędu w Biuletynie Informacji Publicznej

standardowych klauzul umownych i zatwierdzonych kodeksów postępowania i służy wskazaniu sposobu podawania do publicznej wiadomości ww. dokumentów.

Uregulowanie zawarte w art. 39 projektu ma na celu określenie formy prawnej podawania przez Prezesa Urzędu do wiadomości publicznej wykazu rodzajów operacji przetwarzania danych osobowych podlegających wymogowi dokonania oceny skutków dla ochrony danych. Przyjmuje się, iż wykaz ten będzie często aktualizowany, stąd forma jego ogłoszenia musi umożliwiać jego bieżącą aktualizację.

Celem art. 40 jest zapewnienie sprawności i zakończenia w rozsądnym czasie postępowania dotyczącego uprzednich konsultacji, o których mowa w art. 36 Rozporządzenia. Przepis ust. 2 art. 36 Rozporządzenia daje organowi nadzorczemu (Prezesowi Urzędu) termin 8 tygodni na przedstawienie zaleceń i ewentualnie skorzystanie z uprawnień przewidzianych w art. 58 Rozporządzenia. Termin ten może być wydłużony o 6 tygodni. Wreszcie bieg tych terminów można zawiesić do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji. W opinii projektodawcy nie wskazanie terminu zawieszenia postępowania może doprowadzić, w skrajnym przypadku, do sytuacji gdy zalecenia nigdy nie zostaną wydane a administrator nie będzie mógł przystąpić do przetwarzania danych. Celem tego przepisu jest zatem zapewnienie administratorom prawa do rozpatrzenia ich sprawy przez Prezesa Urzędu w rozsądnym terminie. W ocenie projektodawcy maksymalny termin 16 tygodni jest wystarczający na sformułowanie zaleceń i ewentualnie skorzystanie z uprawnień przewidzianych w art. 58 Rozporządzenia.

Celem przepisu art. 42 jest określenie, iż dla czynności w nim wymienionych przyjmuje się formę decyzji administracyjnej. Wprowadzenie tej formy rozstrzygnięcia Prezesa Urzędu ma na celu zapewnienie odpowiedniego poziomu ochrony stron postepowania. Przy wydawaniu tych decyzji zastosowanie będą miały przepisy o postępowaniu zawarte w Rozdziale 5 projektu, z wyłączeniem art. 53 dotyczącego wydawania postanowień dotyczących ograniczenia przetwarzania danych osobowych i art. 55 dotyczącego rodzaju rozstrzygnięć wydawanych w toku postepowania. Wyłączenie wynika z tego, iż ww. przepisy nie znajdą zastosowania w sprawach wymienionych w art. 42.

Przepisy art. 43 projektu nakłada na Prezesa Urzędu obowiązek opracowywania i udostępniania rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Zgodnie z art. 32 ust. 1 Rozporządzenia uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i

podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Ww. przepis jest wyrazem zastosowania w Rozporządzeniu podejścia *risk based approach*, a więc podejścia opartego na ryzyku administratora lub podmiotu przetwarzającego. To już nie przepisy prawa powszechnie obowiązującego mają określać środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych ale sami administratorzy lub podmioty przetwarzające. Stosowane środki powinny być zawsze dopasowywane do okoliczności i ryzyk związanych z przetwarzaniem danego rodzaju danych osobowych. Tym niemniej w ocenie projektodawcy, by zapewnić administratorom i podmiotom przetwarzającym wsparcie w określaniu takich środków, uzasadnione jest, by Prezes Urzędu opracowywał i udostępniał rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Rekomendacje takie powinny być wypracowane przy współpracy z zainteresowanymi podmiotami, których zakresu działania dotyczy dany projekt – w tym izbami gospodarczymi. Rekomendacje nie będą miały mocy wiążącej, ale będą stanowiły punkt odniesienia dla przedsiębiorców, wpływając w ocenie projektodawcy na podwyższenie poziomu ochrony danych osobowych.

Przepisy **Rozdziału 5** projektu ustawy regulują sposób postępowania w sprawach naruszenia przepisów o ochronie danych osobowych. Należy przede wszystkim podkreślić, iż mówiąc o naruszeniu przepisów o ochronie danych osobowych projektodawca odnosi się nie tylko do naruszeń ustawy ale również przepisów Rozporządzenia, z których w sposób bezpośredni wynikają określone prawa i obowiązki podmiotów danych osobowych, administratorów lub podmiotów przetwarzających.

Na gruncie obowiązującej Ustawy postępowanie w sprawach naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", prowadzi się według przepisów Kodeksu postepowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej. Zasada stosowania w sprawach nieuregulowanych Kodeksu postepowania administracyjnego została zachowana w projekcie. Projektodawca nie zdecydował się na wprowadzenie odrębnego, właściwego dla naruszeń ochrony danych osobowych, trybu postępowania przed Prezesem Urzędu. U podstaw takiej decyzji legło przekonanie, iż obowiązująca procedura administracyjna, z odmiennościami wynikającymi choćby z bezpośredniego stosowania Rozporządzenia, zapewnia kompletny a zarazem sprawdzony w praktyce mechanizm postępowania. Postępowania prowadzone przez Prezesa Urzędu będą postępowaniami w sprawie naruszenia prawa podstawowego, a stronom tak prowadzonych postępowań przysługiwać powinien pełen katalog uprawnień procesowych przewidzianych w Kodeksie.

Wyłączenie stosowania Kodeksu i próba stworzenia szczególnego postępowania w sprawie naruszenia przepisów o ochronie danych obarczona byłaby z jednej strony ryzykiem nie uregulowania niezbędnych elementów postępowania a z drugiej koniecznością tworzenia obszernej listy przepisów Kodeksu, które jednak znalazłyby zastosowanie w postępowaniu. Działania takie uznano za nieracjonalne.

Postępowanie będzie prowadzone przez Prezesa Urzędu jako organ właściwy w sprawie ochrony danych osobowych. Korzystając z możliwości przewidzianej w Konstytucji RP oraz w Kodeksie projektodawca przewidział jednoinstancyjność postępowania. Odnosząc się do projektowanego rozwiązania należy zauważyć, że konstytucyjna zasada zaskarżalności orzeczeń i decyzji wydanych w pierwszej instancji „(…) obejmuje swym zakresem nie tylko postępowanie sądowe, ale również administracyjne oraz inne postępowania, w których organ władzy publicznej wydaje akt kształtujący sytuację prawną podmiotu praw i wolności" (wyrok TK z dnia 6 grudnia 2011 r. SK 3/11). Jednocześnie, zasada dwuinstancyjności nie ma charakteru absolutnego, na co wskazuje sam art. 78 zdanie drugie Konstytucji, a zatem ustawodawca może wprowadzać wyjątki od tej zasady, wprowadzając określone postępowanie jednoinstancyjnym. Zasady ustanawiania takich wyjątków nakreślił Trybunał Konstytucyjny m.in. w uzasadnieniu wyroku z dnia 12 czerwca 2002 r., P 13/01, wskazując, że „Powinny być one ustalone w ustawie. Konstytucja nie precyzuje charakteru tych wyjątków, nie wskazuje bowiem ani zakresu podmiotowego, ani przedmiotowego, w jakim odstępstwo od tej zasady jest dopuszczalne. Nie oznacza to jednak, iż ustawodawca ma pełną, niczym nieskrępowaną swobodę w ustalaniu katalogu takich wyjątków. W pierwszym rzędzie należy liczyć się z tym, iż nie mogą one prowadzić do naruszenia innych norm konstytucyjnych. (…) [ponadto] odstępstwo od reguły wyznaczonej treścią normatywną art. 78 Konstytucji w każdym razie powinno być podyktowane szczególnymi okolicznościami, które usprawiedliwiałyby pozbawienie strony postępowania środka odwoławczego". Zgodnie z dominującym stanowiskiem Trybunału wyjątki od zasady dwuinstancyjności powinny również czynić zadość wymaganiom stawianym przez zasadę proporcjonalności (art. 31 ust. 3 Konstytucji; wyroki TK: z dnia 17 lutego 2004 r., SK 39/02; z dnia 18 kwietnia 2005 r., SK 6/05; z dnia 14 października 2010 r., K 17/07).

Przewidziany przez projektodawcę wyjątek od zasady dwuinstancyjności postępowania administracyjnego jest, w jego ocenie, konieczny w demokratycznym państwie dla zapewnienia wolności i praw osób. Jest to rozwiązanie adekwatne i konieczne dla osiągnięcia celu zamierzonego przez ustawodawcę, jakim jest skuteczna i udzielona we właściwym czasie ochrona prawa podstawowego - prawa do ochrony danych osobowych osoby fizycznej oraz pozostaje w odpowiedniej proporcji do ograniczenia, jakim jest pozbawienie prawa do

ponownego rozpatrzenia sprawy przez właściwy organ. Za wprowadzeniem jednoinstancyjności postępowania przemawia konieczność zapewnienia osobie, której prawa zostały naruszone ostatecznego rozstrzygnięcia (ostatecznej decyzji administracyjnej), które będzie mogło być skutecznie i szybko egzekwowalne. Tak więc w ocenie projektodawcy ochrona danych osobowych osoby fizycznej wymaga by zasadą była natychmiastowa wykonalność takich decyzji. Ochrona wartości, jaką są dane osobowe osoby fizycznej, wymaga natychmiastowego działania inaczej często traci swój sens, gdyż z upływem czasu naruszenia mogą mieć miejsce na wielką skalę a ich skutki nieodwracalny charakter.

Warto również podkreślić, że w postępowaniu prowadzonym przez Prezesa Urzędu nie mamy do czynienia z odwołaniem składanym do organu wyższego stopnia lecz z wnioskiem o ponowne rozpatrzenie sprawy, który rozpatrywany jest przez ten sam organ. Jak pokazują statystyki dotyczące decyzji wydawanych w postępowaniach w wyniku wniosku o ponowne rozpatrzenie sprawy, decyzje wydawane po ponownym rozpatrzeniu sprawy w zdecydowanej większości nie prowadzą do zmiany rozstrzygnięć wydawanych w pierwszej instancji przez organ właściwy w sprawie ochrony danych osobowych.

Należy podkreślić, iż rozstrzygnięcia wydawane przez Prezesa Urzędu jako organ właściwy w sprawie ochrony danych osobowych będą podlegały zaskarżeniu do sądu administracyjnego i skargi w tych sprawach będą podlegały dwuinstancyjnemu postępowaniu sądowoadministracyjnemu. Powyższe oznacza, iż prawa podmiotów danych osobowych i innych stron postępowania przed Prezesem Urzędu do wnikliwego rozpatrzenia sprawy i sądowej kontroli rozstrzygnięć administracji zostaną zapewnione. Nie zostaje również wyłączone prawo strony takiego postępowania do żądania wstrzymania wykonalności decyzji lub postanowienia.

Wprowadzenie zasady jednoinstancyjności postępowania służy realizacji celów zakładanych przez ustawodawcę, jakimi są zapewnienie adekwatnej i skutecznej ochrony praw osób, których prawo do ochrony danych osobowych zostało naruszone i cele te są uzasadnione w świetle wartości wymienionych w art. 31 ust. 3 Konstytucji. Jednoinstancyjność postępowania nie narusza bowiem prawa strony postępowania do kontroli rozstrzygnięcia wydawanego przez Prezesa Urzędu, nie narusza zatem istoty prawa, jaką jest konieczność ponownego, wnikliwego, niezależnego zbadania jej sprawy. W ocenie projektodawcy wprowadzenie ww. zasady jest niezbędne dla ochrony wartości, jaką jest prawo do ochrony danych osobowych i nie można uznać jej wprowadzenia, biorąc pod uwagę ww. argumenty, za środek nadmiernie „restrykcyjny”. Efekt wprowadzenia omawianej regulacji, a więc zapewnienie skutecznej ochrony podmiotom danych osobowych polegającej choćby na zatrzymaniu nieuprawnionego

przekazywania danych osobowych osoby fizycznej do państw trzecich ma wartość większą niż wartość wynikająca z ponownego rozpatrzenia sprawy przez ten sam organ administracyjny.

Obok jednoinstancyjności kolejną odrębnością postępowania przewidzianego w ustawie w stosunku do postępowania unormowanego w Kodeksie jest rozszerzenie prawa organizacji społecznych do wystąpienia z żądaniem wszczęcia postępowania albo dopuszczenia ich do udziału w postępowaniu. Na gruncie art. 31 Kodeksu organizacja społeczna może w sprawie dotyczącej innej osoby występować z żądaniem: 1) wszczęcia postępowania, 2) dopuszczenia jej do udziału w postępowaniu, jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes społeczny. Przepisy projektowanej ustawy umożliwiają udział organizacji społecznej w postępowaniu także wówczas, gdy organizacja nie może wykazać się istnieniem interesu społecznego w danej sprawie. W sprawach o naruszenie praw przysługujących na mocy przepisów o ochronie danych osobowych wystarczy, jeśli organizacja społeczna uzasadni swój udział w postępowaniu tym, że za jej udziałem przemawia interes osoby, której prawa zostały naruszone. Dodatkową przesłanką udziału organizacji społecznej w postępowaniu, zarówno na gruncie Kodeksu jak i projektowanej ustawy jest istnienie uzasadnienia tego udziału z punktu widzenia celów statutowych organizacji. Powyższa regulacja ma na celu zapewnienie stosowania art. 80 Rozporządzenia.

Kolejny przepis projektowanej ustawy (art. 46) wskazuje, iż organ zawiadamiając strony o każdym przypadku niezałatwienia sprawy w terminie oprócz, jak dotychczas, podania przyczyn zwłoki i nowego terminu załatwienia sprawy jest obowiązany podać także informację o stanie sprawy i przeprowadzonych w jej toku czynnościach. Regulacja ta stanowi modyfikację art. 36 Kodeksu i służy zapewnieniu stosowania art. 78 ust. 2 Rozporządzenia, który stanowi, iż bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 55 i 56 Rozporządzenia nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 77 do organu nadzorczego. Przyjmując, iż zgodnie z Kodeksem rozpatrzenie sprawy szczególnie skomplikowanej powinno nastąpić nie później niż w terminie dwóch miesięcy od dnia wszczęcia postępowania a o każdym przypadku jej niezałatwienia w terminie należy zawiadomić strony, przyjęto iż regulacja art. 46 projektu zapewni stronie postępowania, w terminie trzech miesięcy, od dnia wszczęcia postępowania informację o postępach lub efektach rozpatrywania wniosku przed Prezesem Urzędu. Brak

takiej informacji w terminie trzech miesięcy od dnia wszczęcia postępowania dawał będzie stronie prawo do wniesienia skargi do sądu administracyjnego.

Celem przepisu art. 47 projektu jest jak najpełniejsza realizacja wyrażonej w Kodeksie zasady prawdy obiektywnej, obowiązku wszechstronnego wyjaśnienia okoliczności sprawy oraz zapewnienia sprawności postępowania. Przepis ten pozwala Prezesowi Urzędu wyznaczyć stronie termin na przedstawienie dowodu będącego w jej posiadaniu oraz żądać od strony tłumaczenia dokumentacji sporządzonej w języku obcym. Przepis ten pozwoli również sądom administracyjnym badającym legalność postępowania prowadzonego przez Prezesa Urzędu stwierdzić, czy organ wykorzystał wszelkie przewidziane prawem możliwości w celu wszechstronnego wyjaśnienia danej sprawy.

Projektowany przepis art. 48 służy zapewnieniu stosowania art. 90 Rozporządzenia. Jego celem jest wskazanie wprost w przepisie ustawy, że uprawnienia Prezesa Urzędu podlegają ograniczeniom w zakresie dostępu do informacji ustawowo chronionych. Odnosząc się do brzmienia art. 90 ust. 1 Rozporządzenia uznano za niezbędne i proporcjonalne dla pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy, ograniczenie uprawnień Prezesa Urzędu w odniesieniu do informacji, w tym danych osobowych, ustawowo chronionych.

Kolejne przepisy projektu odnoszą się do możliwości zastrzeżenia informacji, dokumentów lub ich części zawierających tajemnicę przedsiębiorstwa oraz ograniczenia prawa wglądu do materiału dowodowego. Zastrzeżenie tajemnicy przedsiębiorstwa nie ma charakteru bezwzględnego. Prezes Urzędu może je uchylić, jeśli nie są spełnione przesłanki uznania danej informacji za tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2003 r. poz. 1503, z późn. zm.). Powyższa regulacja ma na celu zapewnienie ochrony tych informacji, które w ocenie strony postępowania będącego przedsiębiorcą mają charakter informacji technicznych, technologicznych, organizacyjnych lub też innych posiadających wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

Odnosząc się do ograniczenia prawa wglądu do materiału dowodowego (art. 50) należy podkreślić, że może ono nastąpić tylko wtedy jeśli groziłoby ujawnieniem tajemnicy przedsiębiorstwa lub innych tajemnic prawnie chronionych. Ograniczenie takie może nastąpić tylko na skutek postanowienia Prezesa Urzędu. Celem przepisu jest zapewnienie należytej ochrony tajemnicom ustawowo chronionym przy jednoczesnym badaniu w każdym przypadku przez Prezesa Urzędu zasadności ograniczenia dostępu do materiału dowodowego ze względu na te tajemnice.

Przepis art. 51 projektu stanowi modyfikację przepisu art. 88 Kodeksu. Celem tego przepisu jest zwiększenie z 50 zł do 500 zł wysokości grzywny za nie stawienie się bez uzasadnionej przyczyny jako świadek lub biegły albo bezzasadne odmówienie złożenia zeznania, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej. Zdaniem projektodawcy waga spraw związanych z naruszeniem przepisów o ochronie danych osobowych wymaga zapewnienia sprawności i skuteczności postępowań w tych sprawach. Dolegliwa kara grzywny jest instrumentem temu służącym.

Przepis art. 53 projektu ma na celu zapewnienie Prezesowi Urzędu narzędzia do natychmiastowej interwencji w sytuacji, gdy zostanie uprawdopodobnione, że dalsze przetwarzanie danych osobowych może spowodować poważne i trudne do usunięcia skutki. W takiej sytuacji Prezes Urzędu, w celu zapobieżenia tym skutkom może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych wskazując dopuszczalny zakres tego przetwarzania. Nie zdecydowano o wprowadzeniu do przepisów projektu ustawy instytucji zażalenia na to postanowienie. Postanowienie to jest natomiast zaskarżalne w skardze na decyzję kończącą postępowanie w sprawie. Decyzja ta, zgodnie z art. 35 Kodeksu, powinna zostać wydana niezwłocznie, w sprawie wymagającej postępowania wyjaśniającego nie później niż w ciągu miesiąca, a w sprawie szczególnie skomplikowanej - nie później niż w ciągu dwóch miesięcy od dnia wszczęcia postępowania. Powyższe oznacza, że w przypadku wprowadzenia zażalenia na ww. postanowienie, które musiałoby również zostać przekazane do sądu administracyjnego i przez ten sąd rozpatrzone, czynności związane z rozpatrzeniem tego zażalenie mogłyby zbiec się w czasie z wniesieniem i rozpatrywaniem skargi na decyzję Prezesa Urzędu a w skrajnym przypadku trwać nawet dłużej. Obowiązujące przepisy o postępowaniu sądowoadministracyjnym nie regulują takich sytuacji ani nie rozstrzygają jak powinien zachować się wówczas sąd. Jednocześnie nie budzi wątpliwości, że ww. postanowienie nie może obowiązywać dłużej niż do czasu wydania decyzji kończącej postępowanie w sprawie (art. 53 ust. 2 projektu). Tym samym w ocenie projektodawcy dla zapewnienia spójności obowiązujących regulacji zasadnym jest przyjęte rozwiązanie, iż postanowienie zobowiązujące podmiot do ograniczenia przetwarzania danych osobowych jest zaskarżalne w skardze na decyzję Prezesa Urzędu.

W projekcie ustawy – w zakresie rozstrzygnięć jakie mogą zapaść po przeprowadzeniu postępowania odesłano do art. 58 ust. 2 lit. b-j rozporządzenia 2016/679. Uznano za niecelowe przepisywanie przepisów Rozporządzenia w tym zakresie. Nowym elementem, a jednocześnie modyfikacją przepisów Kodeksu, jest przepis art. 55 ust. 2 projektowanej ustawy, który nakłada na organ obowiązek poszerzenia uzasadnienia decyzji nakładającej na

stronę administracyjną karę pieniężną o wskazanie przesłanek z art. 83 ust. 2 Rozporządzenia. Powyższe ma na celu ułatwienie sądowi oceny legalności samego nałożenia na stronę administracyjnej kary pieniężnej jak i jej wysokości.

Przepis art. 56 projektu ustawy pozwala, w przypadku znikomej wagi naruszenia oraz jego zaprzestania przez stronę, udzielić stronie, w drodze decyzji administracyjnej, upomnienia. Przepis ten ma na celu zapewnienie stosowania art. 58 ust. 2 lit. b Rozporządzenia, który stanowi o uprawnieniu organu nadzorczego do udzielania upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów Rozporządzenia przez operacje przetwarzania danych. W Kodeksie przepis art. 189f § 1 stanowi, że organ administracji publicznej, w drodze decyzji, odstępuje od nałożenia administracyjnej kary pieniężnej i poprzestaje na pouczeniu m.in. jeżeli waga naruszenia prawa jest znikoma, a strona zaprzestała naruszania prawa. W projekcie ustawy zdecydowano się wprowadzić pojęcie upomnienia. W odróżnieniu od Kodeksowego pouczenia upomnienie może być stosowane „obok" administracyjnej kary pieniężnej. Postanowiono jednak przyjąć dla upomnienia takie same przesłanki jak dla Kodeksowego pouczenia.

Przepis art. 57 projektu jest związany z przepisem art. 83 projektu. Przepis art. 57 nakłada na Prezesa Urzędu obowiązek ogłaszania w Biuletynie Informacji Publicznej prawomocnych decyzji administracyjnych zawierających rozstrzygnięcia, o których mowa w art. 58 ust. 2 lit. b – g i lit. j Rozporządzenia, wydanych wobec organów, o których mowa w art. 5 § 2 pkt 3 Kodeksu postępowania administracyjnego albo podmiotów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, zwanych dalej łącznie „podmiotami publicznymi". Podmioty publiczne mają natomiast obowiązek udostępniania na swoich stronach internetowych informacji o działaniach podjętych w celu wykonania ww. decyzji. Celem tej regulacji jest przedstawienie opinii publicznej informacji o ewentualnych naruszeniach przepisów z zakresu ochrony danych osobowych przez podmioty publiczne oraz działaniach podjętych przez nie w celu usunięcia tych naruszeń. Natomiast w przepisie art. 84 projektu ograniczono wysokość administracyjnej kary pieniężnej, którą można nałożyć na podmioty publiczne do 100 000 zł.

Przepis art. 58 stanowi powielenie przepisów obowiązującej ustawy (art. 18 ust. 2a).

Odnosząc się do art. 59 projektu wskazać należy, że decyzje wydane przez Prezesa Urzędu w postepowaniu jednoinstancyjnym są decyzjami ostatecznymi podlegają więc natychmiastowemu wykonaniu. Zgodnie z art. 61 § 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi wniesienie skargi nie wstrzymuje wykonania aktu lub czynności. Wyjątek od tej zasady wprowadza art. 59 ust. 2 projektu, który

stanowi, że wniesienie przez stronę skargi do sądu administracyjnego powoduje wstrzymanie wykonania decyzji w zakresie dotyczącym administracyjnej kary pieniężnej. Przyjęto ustawowe wstrzymanie wykonalności decyzji administracyjnej nakładającej administracyjną karę pieniężną, tak by dopiero po rozpatrzeniu sprawy przez sąd i oddaleniu skargi decyzja taka podlegała wykonaniu. Wynika to oczywiście z dolegliwości administracyjnej kary pieniężnej.

W projekcie ustawy nie przewiduje się zażaleń na postanowienia jako odrębnych środków odwoławczych. Wszystkie postanowienia wydawane w toku postępowania będą podlegały zaskarżeniu w skardze na decyzję Prezesa Urzędu. Zapewni to rozpatrzenie w jednym postępowaniu sadowoadministracyjnym wszystkich spraw związanych z prowadzonym przez Prezesa Urzędu postępowaniem.

Wreszcie ostatnie wyłączenie w odniesieniu do Kodeksu dotyczy przepisu art. 66a Kodeksu. Przepis art. 66a Kodeksu reguluje kwestię zakładania metryki sprawy. Projektodawca uznał, że obowiązek jej prowadzenia w formie wskazanej w Kodeksie można wyłączyć przy założeniu prowadzenia przez Prezesa Urzędu elektronicznego systemu zarządzania dokumentacją, w którym dokumentowane są wszystkie czynności dokonywane w sprawie i osoby ich dokonujące.

Przepisy **Rozdziału 6** ustawy mają zapewnić skuteczne stosowanie rozdziału VII Rozporządzenia regulującego zagadnienia europejskiej współpracy administracyjnej w sprawach ochrony danych osobowych. Mimo, że przepisy proceduralne wprowadzone do rozdziału VII Rozporządzenia są bezpośrednio skuteczne i co do zasady w sposób wyczerpujący regulują zasady prowadzenia współpracy, bez podjęcia krajowej uzupełniającej aktywności ustawodawczej, ich zastosowanie byłoby w polskim porządku prawnym w niektórych obszarach niemożliwe.

Koniecznym było doprecyzowanie formy prawnej działań podejmowanych przez Prezesa Urzędu na podstawie art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 Rozporządzenia. Wszystkie z powołanych przepisów zobowiązują Prezesa Urzędu do wydawania środków tymczasowych, którym w polskim porządku prawnym nadana została forma postanowienia. Zgodnie z motywem 137 Rozporządzenia, organ nadzorczy powinien w razie pilnej potrzeby podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą mieć możliwość przyjmowania na swoim terytorium należycie uzasadnionych środków tymczasowych o określonym czasie obowiązywania. Motyw znajduje swoje odzwierciedlenie w powołanych już art. 61 ust. 8, 62 ust. 7 oraz 66 ust. 1 Rozporządzenia. Nie jest więc możliwe zapewnienie przez ustawodawcę krajowego skutecznego stosowania tych przepisów Rozporządzenia, bez

przyznania Prezesowi Urzędu uprawnienia do wydawania takich środków tymczasowych. Po drugie należy wskazać, że rozwiązanie wprowadzone do projektu ustawy o ochronie danych osobowych nie jest rozwiązaniem obcym polskiemu porządkowi prawnemu. Z podobnymi rozwiązaniami mamy do czynienia chociażby w przypadku zabezpieczenia roszczeń w postępowaniu cywilnym bądź postępowaniu antymonopolowym w przypadku decyzji Prezesa UOKiK zobowiązującej przedsiębiorcę, któremu jest zarzucane stosowanie praktyk monopolowych by w drodze decyzji, zobowiązać go, do zaniechania określonych działań. Skoro praktyki które nie skutkują bezpośrednio naruszeniem praw podstawowych obywateli, zostały poddane takiej instytucji ochronnej, dziwi zamieszanie związane z ich wprowadzeniem w projekcie ustawy o ochronie danych. Po trzecie, zastosowanie przez Prezesa Urzędu takich środków tymczasowych obwarowane jest w projekcie restrykcyjnymi wymogami. Musi dojść do uprawdopodobnienia naruszenia, naruszenie powinno powodować poważne i trudne do usunięcia skutki, środek powinien przewidywać dopuszczalny zakres przetwarzania i czas jego obowiązywania. Zastosowanie tych środków następować powinno więc bez wątpienia wyjątkowo. Prezes Urzędu powinien wskazać również ograniczony zakres przetwarzania danych, nie powinien on jednak rodzić nieodwracalnych skutków jak np. usunięcie przetwarzania danych osobowych. Obawy budzi również brak przewidzenia wprost w projekcie środków zaskarżenia na wydawane przez Prezesa Urzędu postanowienie. Organem właściwym do rozpatrzenia takiego środka powinien być sąd, uwzględniając jednak krótkie wynikające z Kodeksu terminy do rozstrzygnięcia sprawy przez Prezesa Urzędu, rozstrzygnięcie sądu mogłoby nastąpić później, niż wydanie rozstrzygnięcia przez Prezesa Urzędu. Nie oznacza to, że przedsiębiorca nie będzie mógł odwołać się od treści środka tymczasowego. Będzie mógł zrobić to w odwołaniu od decyzji wydanej przez Prezesa Urzędu, a wyrok sądu administracyjnego będzie podstawą do ewentualnego dochodzenia odpowiedzialności odszkodowawczej na drodze cywilnej. Przewidziane rozwiązanie, jest również odpowiedzią na sygnalizowaną potrzebę nieraz natychmiastowej reakcji na naruszenie ochrony danych osobowych, gdzie skutki naruszenia odczuwalne są dla obywatela bardzo często każdego dnia, i każdy dzień trwania postępowania przez Prezesa Urzędu wiąże się z poważnymi skutkami.

W Rozporządzeniu brak jest jakichkolwiek regulacji prawnych w zakresie języka prowadzenia współpracy w sprawach ochrony danych osobowych. Należy więc przyjąć, że wszelkie informacje pomiędzy organem a Komisją Europejską, Europejską Radą Ochrony Danych oraz organami nadzorczymi, mogą być przesyłane w każdym z oficjalnych języków UE. Powyższe, stanowi jednak dodatkowy czynnik znacznie utrudniający współpracę w ramach mechanizmu zgodności. O ile bowiem, w ramach aparatu administracyjnego Komisji

Europejskiej zatrudnieni są urzędnicy, władający biegle wszystkimi językami UE, o tyle organy nadzorcze państw członkowskich pracownikami takimi nie dysponują. Art. 6 rozporządzenia Rady nr 1/58 z 15 kwietnia 1958 r. poświęconego językom UE, zwanego „Kartą Języków Unii Europejskiej" przyznaje instytucjom unijnym możliwość wyboru języka, w którym rozpatrywane by były określone kategorie spraw. Działanie takie, mogłoby zostać jednak uznane za sprzeczne z jednym z zadań przed jakim stoi Komisja tj. odpowiedzialność, za upowszechnianie wiedzy na temat wielojęzyczności i opiekę nad nią - powołana została zresztą w tym celu instytucja Komisarza ds. Wielojęzyczności. W związku z powyższym ustawodawca unijny odstąpił od regulowania jakichkolwiek zagadnień związanych z językiem prowadzonej współpracy. Uwzględniając powyższe, oraz jedną z podstawowych wartości jaką jest wielokulturowość UE, przepisy ustawy nakładają obowiązek kierowania korespondencji przez Prezesa Urzędu w jednym z języków urzędowych państwa członkowskiego będącego adresatem danej czynności lub w języku angielskim. Uwzględniając, że krajowe przepisy o ochronie danych osobowych nie mogą nakładać jakichkolwiek obowiązków na inne państwa członkowskie, art. 64 ust. 2 nakłada na Prezesa Urzędu obowiązek tłumaczenia na język polski wszelkiej formalnej korespondencji doręczanej do niego w ramach mechanizmów współpracy w innym języku, o ile w związku z podejmowanymi czynnościami mogą mieć one jakikolwiek wpływ na sytuację prawną jakiejkolwiek osoby bądź podmiotu. Powyższy przepis dotyczył będzie w szczególności korespondencji doręczanej Prezesowi Urzędu w związku z podejmowanymi przez niego czynnościami kontrolnymi bądź prowadzonym postępowaniem.

Dokonywanie efektywnej współpracy wymaga dokładnego doprecyzowania zakresu zadań podejmowanych przez każdy z organów nadzorczych państw członkowskich. Art. 64 ust. 1 projektu ustawy nakłada wymóg przyjęcia przez Prezesa Urzędu podejmującego wspólne operacje, o których mowa w art. 62 ust. 1 Rozporządzenia, z innymi organami nadzorczymi państw członkowskich wykaz ustaleń dotyczących takich wspólnych operacji. Krajowe przepisy o ochronie danych osobowych nie mogą nakładać obowiązku podejmowania takich działań przez inne państwa członkowskie, adresatem obowiązku jest więc Prezes Urzędu. Rozwiązanie takie nie jest obce polskim przepisom prawnym, i wprowadzone zostało również do art. 5 ust. 1 ustawy z dnia 7 lutego 2014 r. o udziale zagranicznych funkcjonariuszy lub pracowników we wspólnych operacjach lub wspólnych działaniach ratowniczych na terytorium Rzeczypospolitej Polskiej.

W przepisach **Rozdziału 7** uregulowano postępowanie kontrolne. Przepisy tego rozdziału będą miały zastosowanie w przypadku czynności kontrolnych prowadzonych w ramach postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, w przypadku

kontroli planowych jak również kontroli doraźnych. Kontrole będą przeprowadzane przez upoważnionych pracowników Urzędu Ochrony Danych Osobowych. Zakres udzielanych upoważnień do przeprowadzenia kontroli określa art. 68 projektu. Do przeprowadzania kontroli będą również uprawnieni członkowie lub pracownicy organu nadzorczego innego państwa członkowskiego. Projektodawca nie zdecydował się skorzystać z uprawnienia z art. 62 ust. 3 Rozporządzenia i przyznać tym osobom uprawnienie do wykonywania ich własnych uprawnień w zakresie postępowania wyjaśniającego. Osoby te będą wykonywały uprawnienia takie jak przysługują pracownikom Urzędu Ochrony Danych Osobowych.

Dla zapewnienia możliwości przeprowadzenia kontroli pod nieobecność kontrolowanego przewidziano, w art. 68 ust. 2, że upoważnienie do przeprowadzenia kontroli będzie mogło być okazane pracownikowi kontrolowanego lub przywołanemu świadkowi, którym powinien być funkcjonariusz publiczny.

Zakres uprawnień kontrolujących oraz obowiązków kontrolowanych określa art. 69 projektu. Porównując projektowaną regulację do regulacji art. 14 obowiązującej Ustawy należy zauważyć, iż zrezygnowano z ograniczenia czasu przeprowadzania kontroli do godzin 6.00 – 22.00, uznając, iż ochrona danych osobowych może w pewnych sytuacjach wymagać podjęcia nagłych czynności kontrolnych. Postanowiono zatem nie wyłączać z mocy ustawy możliwości przeprowadzenia kontroli poza ww. godzinami.

Ważną i nową regulacją, mająca na celu skuteczne przeprowadzenie czynności kontrolnych, jest przepis art. 69 ust. 4 pozwalający kontrolującym korzystać z pomocy funkcjonariuszy innych organów kontroli lub Policji.

Przebieg przeprowadzonej kontroli kontrolujący przedstawi w protokole kontroli. Zawartość tego protokołu określa art. 72 ust. 2 projektu. Zasadą jest, iż protokół podpisują kontrolujący i kontrolowany. W przypadku odmowy podpisania protokołu przez kontrolowanego, kontrolujący czyni o tym wzmiankę w protokole.

Przepis art. 73 projektu przewiduje stosowanie do postępowania kontrolnego w przypadku kontroli działalności gospodarczej przedsiębiorcy przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, z wyjątkiem przepisów art. 79, 82 i 83. Powyższe oznacza, że nie będą miały zastosowania do kontroli przestrzegania przepisów o ochronie danych osobowych przepisy dotyczące zawiadomienia o zamiarze wszczęcia kontroli, zakazu podejmowania i prowadzenia więcej niż jednej kontroli działalności przedsiębiorcy oraz ograniczeń w zakresie czasu trwania wszystkich kontroli organu kontroli u przedsiębiorcy w jednym roku kalendarzowym. W opinii projektodawcy zastosowanie ww. przepisów mogłoby

uniemożliwić rzetelne i przeprowadzone we właściwym czasie postępowanie kontrolne w zakresie przestrzegania przepisów o ochronie danych osobowych. Trudno bowiem sobie wyobrazić, że kontrola doraźna w ww. zakresie nie mogłaby się odbyć z uwagi np. na trwającą kontrolę przestrzegania przepisów z zakresu ochrony środowiska. Ochrona prawa podstawowego jakim jest prawo do ochrony danych osobowych mogłaby wówczas stać się iluzją.

Nową i ważną regulacją, mając na uwadze obecną praktykę, jest przepis art. 74 projektu, który przewiduje, że postępowanie kontrolne nie może trwać dłużej niż miesiąc od dnia podjęcia czynności kontrolnych. Przy czym za podjęcie czynności kontrolnych należy uznać moment, w którym kontrolujący okazuje kontrolowanemu, lub innej osobie wskazanej w przepisach, upoważnienie do przeprowadzenia kontroli oraz legitymację służbową lub inny dokument potwierdzający tożsamość. Celem tego przepisu jest ograniczenie w czasie czynności kontrolnych prowadzonych przez organ, tak by dla podmiotów kontrolowanych nie istniała uciążliwość oraz niepewność związana z długotrwałym prowadzeniem tego postępowania. Co ważne za dzień zakończenia postępowania kontrolnego przyjęto dzień podpisania protokołu przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 72 ust. 7.

Kolejną nową w porównaniu z obowiązującą Ustawą i ważną regulacją jest przepis art. 74 ust. 3 projektu. Stanowi on, że czasu trwania postępowania kontrolnego nie wlicza się do terminów załatwiania spraw przewidzianych w art. 35 Kodeksu. Powyższe oznacza, że w przypadku prowadzenia przez organ w ramach postępowania czynności kontrolnych, to termin załatwienia sprawy przewidziany w art. 35 Kodeksu może się wydłużyć maksymalnie o miesiąc. Celem regulacji jest zapewnienie Prezesowi Urzędu właściwego czasu na rzetelne przeprowadzenie i udokumentowanie czynności kontrolnych oraz wszechstronne zbadanie i rozpatrzenie okoliczności sprawy. Powyższe nabiera szczególnego znaczenia w kontekście art. 83 Rozporządzenia, który przewiduje możliwość nałożenia na administratorów lub podmioty przetwarzające wysokich administracyjnych kar pieniężnych.

Rozdział 8 (art. 78-81) projektu ustawy odnosi się do odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych.

Art. 78 projektu wdraża do polskiego porządku prawnego regulację art. 79 ust. 1 Rozporządzenia. Zgodnie z treścią tego przepisu:

„1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda

osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia.”.

Art. 79 ust. 1 Rozporządzenia wymaga od państw członkowskich, aby w ich systemach prawnych istniały skuteczne środki ochrony prawnej przed sądem w przypadku gdy podmiot danych uzna, że prawa przysługujące mu na mocy Rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia. Art. 79 ust. 1 Rozporządzenia dotyczy zarówno środków o charakterze materialnoprawnym jak i procesowym.

Art. 79 ust. 1 Rozporządzenia nie wymaga wprowadzenia do systemu prawa państwa członkowskiego nowego środka na płaszczyźnie prawa materialnego, jeżeli obowiązujące przepisy mogą stanowić skuteczną podstawę roszczeń związanych z naruszeniem ogólnego rozporządzenia (czy ogólnie przepisów o ochronie danych osobowych).

W tym miejscu należy zwrócić uwagę, iż realizacja normy kompetencyjnej wskazanej w art. 79 ust. 1 Rozporządzenia nie może naruszać bezpośrednio skutecznej normy wyrażonej w art. 82 Rozporządzenia (tj. nie może ograniczać dochodzenia roszczeń w oparciu o tę podstawę prawną). Zgodnie z treścią art. 82 ust. 1 Rozporządzenia każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego Rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. W art. 82 ust. 1 Rozporządzenia chodzi więc o roszczenia majątkowe (art. 82 ust. 5 Rozporządzenia mówi o „zapłacie” odszkodowania), które można dochodzić w razie zaistnienia szkody majątkowej lub niemajątkowej (zob. M. Gumularz, Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich, Europejski Przegląd Sądowy z 2017, nr 5).

W związku z powyższym projektowany art. 78 nie dotyczy roszczeń odszkodowawczych, które mogą być realizowane w przypadku poniesienia szkody majątkowej lub niemajątkowej w wyniku naruszenia przepisów Rozporządzenia w oparciu o art. 82 Rozporządzenia.

Art. 78 ust. 2 projektu wyraźnie przesądza, iż dochodzenie roszczeń w oparciu o art. 78 projektu nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych. Celem tej regulacji jest m.in. rozstrzygnięcie

ewentualnych wątpliwości, które mogłyby dotyczy relacji pomiędzy art. 78 projektu oraz art. 82 Rozporządzenia.

W doktrynie i orzecznictwie, nie budzi wątpliwości, iż naruszenie danych osobowych stanowi jednocześnie naruszenie dóbr osobistych. Art. 23 k.c. zawiera otwarty katalog dóbr osobistych. Natomiast dane osobowe ujmowane są jako kategoria dobra osobistego - prywatności. Dane osobowe nie mają więc charakteru samoistnego dobra osobistego (tak P. Sobolewski, Kodeks cywilny. Komentarz. Tom I. Przepisy wprowadzające. Część ogólna. Własność i inne prawa rzeczowe, K. Osajda (red.), Warszawa jako: „sfera fizycznej przestrzeni, a także myśli i przeżyć człowieka oraz informacji o nim, do której dostęp można uzyskać tylko za jego zgodą (przy czym zakres ochrony tej sfery może być różny ze względu na pełnioną przez daną osobę rolę społeczną)" (P. Machnikowski, Kodeks cywilny. Komentarz, E. Gniewek, P. Machnikowski (red.), Warszawa 2016, komentarz do art. 23 k.c., teza 2). Jednocześnie w piśmiennictwie podkreśla się, iż „Prywatność jest pojęciem wieloznacznym, trudnym do zdefiniowania. W wyjaśnieniach doktryny dotyczących istoty prywatności zwraca się zwłaszcza uwagę na aspekt poszanowania prawa człowieka do odosobnienia się, pozostawienia w spokoju, co przekłada się na ujęcie prywatności jako obszaru niedostępności, wolnego od ingerencji zewnętrznej, stwarzającego warunki do swobodnego kształtowania własnego życia i rozwoju własnej osobowości. Wskazuje się również, w nawiązaniu do przepisów konstytucyjnych, że za istotny komponent prywatności należy uznać autonomię człowieka w decydowaniu o swoim życiu osobistym (art. 47 Konstytucji RP), a także autonomię informacyjną" (Panowicz-Lipska, Kodeks cywilny. Komentarz. Księga I. Część ogólna, J. Gutowski (red.), Warszawa 2016, komentarz do art. 23 k.c., teza 13).

Przedstawione rozumienie dobra osobistego tj. prywatności rodzi ryzyko wąskiego ujęcia w jej ramach danych osobowych (m.in. pojawia się wątpliwość czy w ramach art. 24 § 1 k.c. można żądać, ażeby osoba, która dopuściła się naruszenia np. odmówiła wydania kopii danych, dopełniła czynności potrzebnych do usunięcia jego skutków). W związku z tym projektodawca zdecydował się na wprowadzenie regulacji odrębnej w art. 78 ust. 1 projektu, dającej wyraźną cywilnoprawną podstawę roszczeń o charakterze niemajątkowym. Dochodzenie roszczeń powiązano z naruszeniem praw podmiotów danych wynikających z przepisów o ochronie danych osobowych (nie tylko Rozporządzenia). W ten sposób, bez potrzeby definiowania dobra osobistego (danych osobowych) skonstruowano podstawę dochodzenia cywilnoprawnych roszczeń niemajątkowych w razie naruszenia praw przysługujących na podstawie przepisów o ochronie danych osobowych.

Należy zwrócić w tym miejscu uwagę, iż art. 78 ust. 1 projektu dotyczy wyłącznie dokonanego naruszenia praw przysługujących na mocy przepisów o ochronie danych osobowych. W tej sytuacji przysługiwać będzie roszczenie o:

- zaniechanie tego działania;

- to aby ten kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków.

Projektowany art. 79 ust. 1 ma charakter porządkowy i przesądza cywilnoprawny tryb dochodzenia roszczeń wskazanych w art. 78 projektu. Natomiast celem art. 79 ust. 2 jest przyznanie sądom okręgowym właściwości w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w tym roszczeń z tytułu art. 82 Rozporządzenia. W związku z tym sądy okręgowe będą właściwe w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, niezależnie od tego czy chodzić będzie o roszczenia majątkowe (niezależnie od wartości przedmiotu sporu) czy niemajątkowe. Przepis ten stanowi regulację szczególną względem art. 17 pkt 4 kodeksu postępowania cywilnego.

Celem wprowadzenia art. 80 oraz 81 projektu jest udrożnienie i przyspieszenie komunikacji pomiędzy sądami powszechnymi a Prezesem Urzędu. Należy zwrócić uwagę, iż wniesienie pozwu w sprawach, o których mowa w art. 78 projektu obliguje sąd – przed którym toczy się postępowanie - do zawiadomienia Prezesa Urzędu. Niemniej sąd może ale nie musi zawiesić toczącego się przed nim postępowania.

Przepisy **Rozdziału 9** projektu dotyczą administracyjnych kar pieniężnych. W pierwszej kolejności należy wskazać, iż przesłanki ich nakładania i maksymalne wysokości wynikają wprost z Rozporządzenia (art. 83 ust. 1 – 6). Odnosząc się do katalogu podmiotów, na które takie kary mogą być nakładane, prawodawca unijny wprowadził możliwość szczególnego uregulowania przez państwa członkowskie kwestii nakładania tych kar na organy i podmioty publiczne (art. 83 ust. 7). Zgodnie bowiem z tym przepisem każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

Na gruncie projektu ustawy przyjęto, iż w polskim systemie prawnym przez organy publiczne będą rozumiane organy administracji publicznej w rozumieniu art. 5 § 2 pkt 3 Kodeksu, a więc: ministrowie, centralne organy administracji rządowej, wojewodowie, działające w ich lub we własnym imieniu inne terenowe organy administracji rządowej (zespolonej i niezespolonej), organy jednostek samorządu terytorialnego oraz organy i podmioty

wymienione w art. 1 pkt 2 Kodeksu. Przez podmioty publiczne będziemy natomiast rozumieli podmioty sektora finansów publicznych a więc:

1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;

2) jednostki samorządu terytorialnego oraz ich związki;

2a) związki metropolitalne;

3) jednostki budżetowe;

4) samorządowe zakłady budżetowe;

5) agencje wykonawcze;

6) instytucje gospodarki budżetowej;

7) państwowe fundusze celowe;

8) Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;

9) Narodowy Fundusz Zdrowia;

10) samodzielne publiczne zakłady opieki zdrowotnej;

11) uczelnie publiczne;

12) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;

13) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

Polski prawodawca skorzystał z możliwości jaką daje art. 83 ust. 7 Rozporządzenia i w przepisie art. 83 postanowił, że kary mogą być nakładane jedynie na podmioty wymienione w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych i wysokość kar nie może przekroczyć 100 000 zł.

Przede wszystkim trzeba zauważyć, że podmioty publiczne są finansowane ze środków budżetu państwa a środki z administracyjnych kar pieniężnych stanowią dochód budżetu państwa. A zatem w przypadku nałożenia na podmiot publiczny administracyjnej kary pieniężnej środki z tej kary pośrednio trafiałyby z powrotem do tego podmiotu. O ile bowiem

w odniesieniu do podmiotów spoza administracji publicznej administracyjna kara pieniężna jest dotkliwą sankcją to nie można zgodzić się, iż taki sam skutek odnosiła ona będzie w stosunku do podmiotów publicznych. Zatem kara ta nie spełniałyby swego represyjnego celu. Dodatkowo nakładanie kar na administrację publiczną w znacznych ilościach pośrednio obciąża obywateli uwzględniając, że środki publiczne pochodzą również z obciążeń podatkowych wnoszonych przez obywateli.

Projektodawca zdecydował się również wprowadzić wyjątek w zakresie nakładania administracyjnych kar finansowych, wyłączając z możliwości objęcia takimi karami państwowe i samorządowe instytucje kultury. Warto, przy tym pamiętać, że Konstytucja Rzeczypospolitej Polskiej wprowadza dwie ważne zasady działania państwa w tej dziedzinie:

- zasadę upowszechniania dóbr kultury, mającą istotne znaczenie dla poznawania kultury, uczestniczenia w niej, tworzenia wspólnoty narodowej oraz procesu patriotycznego wychowania i kształtowania postaw obywatelskich,

- zasadę zapewnienia równego dostępu do tych dóbr, które stanowią źródło tożsamości Narodu, jego trwania i rozwoju.

Realizacja ww. zasad następuje, w formie działań niewładczych, nie może wręcz ze względu na swój charakter być zabezpieczona przymusem administracyjnym. Uczestniczenie w kulturze, jako jej odbiorca, animator, czy twórca, tj. kreowanie usług kulturalnych czy korzystanie z usług kulturalnych jak i z mecenatu państwa ma charakter dobrowolny i niekiedy wiąże się z koniecznością umożliwienia przetwarzania danych osób korzystających z ofert największego mecenasa kultury jakim jest państwo i jego instytucje. Państwowe i samorządowe instytucje kultury, a także jednostki zakładane i prowadzone przez osoby fizyczne czy fundacje i stowarzyszenia, dysponują z reguły niewielkimi budżetami, a jednocześnie zakres przetwarzanych danych osobowych nie powoduje znaczącego zagrożenia dla prywatności użytkowników. Muzea, teatry i podobne instytucje zwykle przetwarzają podstawowe dane osobowe, takie jak: imię, nazwisko, adres i dane kontaktowe. Dane te są potrzebne najczęściej w związku z korzystaniem z karnetów, newsletterów, itp. usług. Dane tego rodzaju są zresztą coraz częściej ogólnodostępne w sieci i służą zapewnieniu dostępu do oferty kulturalnej, zachęceniu do korzystania z niej, zaktywizowaniu i promowaniu działań animatorskich czy twórczych. Zagrożenie wysokimi karami administracyjnymi w ocenie projektodawcy zniechęciłoby do prowadzenia tego typu działalności, a tym samym pozbawiłoby, a w każdym razie znacznie ograniczyło, obywatelom możliwość dostępu do kultury, w szczególności w wymiarze lokalnym. Tam gdzie realne nakłady na kulturę są najniższe (gminy wiejskie czy małe miasta) i funkcjonują najbardziej podstawowe formy

działalności kulturalnej (tj. biblioteka gminna i ośrodek kultury, a często wspólna biblioteka gminy i powiatu czy biblioteka i ośrodek połączone w jedną instytucję, tak aby jak najwięcej środków wydatkowanych było wyłącznie na samą działalność kulturalną, a nie jej obsługę czy administrowanie nią) trudno byłoby zaakceptować dodatkowe obciążenia finansowe, wynikające z kar stanowiących znaczący ułamek rocznego budżetu instytucji. Z kolei, należy też wskazać, że co do zasady kultura jest traktowana, w wielu regulacjach ustrojowych, administracyjnych, karnych, cywilnoprawnych czy finansowo –podatkowych w sposób szczególny, zwłaszcza w zestawieniu z innymi sferami działalności czy usług publicznych, i to tak w zakresie prawa unijnego jak krajowego. Przykładowo, do działalności kulturalnej w pewnym zakresie nie stosuje się w ogóle Prawa zamówień publicznych (art. 4d ust. 1 pkt 2 tej ustawy). Ponadto ogranicza się jawność informacji związanych z postępowaniem o udzielenie zamówienia dostaw lub usług z zakresu działalności kulturalnej (art. 8 ust.4 rzeczonej ustawy) czy wprowadza bardziej złagodzony reżim udzielania zamówień (taki jak do innych tzw. usług społecznych), który oddaje inicjatywę w zakresie kształtu postępowania zamawiającemu (art. 138p i nast. ustawy). Takie uproszczenia czy wyłączenia w ramach procedur przy udzielaniu zamówień na dostawy czy usługi z zakresu kultury, mają swoje umocowanie w prawodawstwie unijnym – vide np. motyw 113, art. 4, art. 21 i art. 74 oraz załącznik XIV dyrektywy 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE tzw. dyrektywy klasycznej albo załącznik XVII dyrektywy 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającej dyrektywę 2004/17/WE z dnia 28 marca 2014 r. – tzw. dyrektywy sektorowej. Kultura i dziedzictwo kulturowe są również szczególnie traktowane w przepisach o pomocy publicznej. Rozporządzenie Komisji (UE) NR 651/2014 z dnia 17 czerwca 2014 r. uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu nie wyłącza wprawdzie kultury spod reguł dotyczących pomocy publicznej, jednakże znacząco ogranicza ich stosowanie w tej dziedzinie. Przykładowo, pod pewnymi warunkami, pomoc na kulturę i zachowanie dziedzictwa kulturowego jest uznana za zgodną z rynkiem wewnętrznym i wyłączona z obowiązku zgłoszenia. Dotyczy to m. in. pomocy udzielanej takim jednostkom jak „muzea, archiwa, biblioteki, ośrodki lub przestrzenie kulturalne i artystyczne, teatry, opery, sale koncertowe, inne organizacje, wystawiające widowiska sceniczne, instytucje odpowiedzialne za dziedzictwo filmowe oraz inne podobne infrastruktury, organizacje i instytucje kulturalne i artystyczne” (art. 53 ust.2 pkt a). Niezależnie od regulacji szczegółowych warto przypomnieć, że artykuł 167 Traktatu o Unii Europejskiej uznaje znaczenie, jakie dla Unii i państw członkowskich ma wspieranie

kultury, oraz stanowi, że Unia powinna uwzględniać aspekty kulturalne w swoim działaniu, zwłaszcza w celu poszanowania i popierania różnorodności jej kultur. Również ostatnio Unia Europejska przystąpiła do prac nad zrewidowaniem stawek podatku VAT na tzw. e-booki. Komisja Europejska przedstawiła pakiet rozwiązań „mających na celu poprawę warunków prowadzenia działalności przez przedsiębiorstwa zajmujące się handlem elektronicznym pod względem podatku VAT". Te działania także wskazują na znaczenie i szczególne podejście UE do spraw kultury. Komisja Europejska przedłoży wniosek dotyczący dyrektywy Rady zmieniającej dyrektywę 2006/112/WE w odniesieniu do stawek podatku od wartości dodanej stosowanego do książek, gazet i czasopism (projekt Komisji Europejskiej z 1 grudnia 2016 r., COM(2016) 758 final). Projekt ten zapowiedziany został w komunikacie Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego dotyczącym planu działania w sprawie VAT (zob. COM(2016) 148 final). W uzasadnieniu do wniosku Komisja wskazuje w szczególności, że „mimo że istnieją różnice między publikacjami drukowanymi i publikacjami elektronicznymi pod względem formatu, oba rodzaje publikacji oferują taką samą treść czytelniczą dla nabywców". Można zatem oczekiwać, że nowa koncepcja zmian dotyczących stawek VAT w sektorze handlu elektronicznego, poskutkuje w efekcie zrównaniem stawek VAT na książki papierowe i ebooki. Z kolei polski ustawodawca w ramach ustawy o organizowaniu i prowadzeniu działalności kulturalnej, gwarantuje instytucjom kultury - jak najdalej możliwą w sferze publicznej - samodzielność prawną, organizacyjną i finansową, przyznając im status osób prawnych (vide art. 14). Zabezpiecza obowiązek finansowania przez organizatorów (art. 12) oraz samodzielność w działaniu (art. 15-17 i art. 27), tak aby instytucje te mogły przede wszystkim realizować zadania związane z upowszechnianiem i ochroną kultury, wspieraniem i promowaniem twórczości, edukacją i oświatą kulturalną czy działaniami i inicjatywami kulturalnymi - w sposób jak najmniej obciążony typowymi dla administracji wymaganiami czy rygorami. W sferze podatkowej polski ustawodawca przewiduje natomiast specjalne rozwiązania promujące twórców i artystów oraz wydatki na cele kulturalne, w tym darowizny (vide art. 21 ust.1 pkt 68 i 132, art. 22 ust. 9 pkt 3 i art. 26 ust.1 lit. a ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych czy art. 18 ust.1 pkt 1 ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych). Analogicznie w systemie ubezpieczeń społecznych artyści i twórcy posiadają pewne preferencyjne rozwiązania emerytalne (vide art. 8 ust. 5 pkt 2, ust.7 i 9, art. 36 ust. 4a, art. 47 ust. 1a ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych oraz art. 6 ust.2 pkt 9 lit.b ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych). Z powyższych powodów w ocenie projektodawcy za zasadne należy szczególne potraktowanie

działalności kulturalnej, w tym prowadzonej przez instytucje kultury, w przepisach o ochronie danych osobowych poprzez wyłączenie stosowania w stosunku do nich administracyjnych kar pieniężnych.

Nową instytucją w polskim systemie prawnym jest Fundusz Ochrony Danych Osobowych będący państwowym funduszem celowym. Przychodami Funduszu ma być 1% administracyjnych kar pieniężnych a wydatki Funduszu mają być przeznaczane na cele wskazane w art. 87 ust. 4 projektu. Celem powołania tej instytucji jest zapewnienie finansowania przedsięwzięć oraz udostępnianie wiedzy z zakresu ochrony danych osobowych.

Rozdział 10 projektu wprowadza do projektu przepisy karne. Generalnie celem projektodawcy było nie rozbudowywanie przepisów karnych i ich ograniczenie do niezbędnych z punktu widzenia systemu ochrony danych osobowych. Wprowadzone do projektu regulacje nie są więc kopią obecnych rozwiązań. Obowiązujące dziś przepisy wskazują wiele czynów zabronionych, ale jednocześnie zbyt ogólnie opisują znamiona poszczególnych z nich. W konsekwencji prokuratorzy i sądy niechętnie sięgają do tych regulacji, co z kolei przekłada się na niewielką liczbę prowadzonych postępowań. Odpowiedzialność karna ma być jednak wyjątkiem przewidzianym wyłącznie dla najcięższych naruszeń przepisów. Będzie stanowiła uzupełnienie dla szeroko uregulowanej odpowiedzialności administracyjnej i cywilnej, a nie główną oś gwarancji przestrzegania przepisów jak obecnie. Przyjęto więc, iż podstawowymi „sankcjami" za naruszenie przepisów o ochronie danych osobowych są nakładane na administratora lub podmiot przetwarzający obowiązki wynikające z prawa administracyjnego oraz administracyjne kary pieniężne. Tym niemniej dla zapewnienia skuteczności systemu ochrony danych osobowych przewidziano sankcję karną za udaremnianie lub utrudnianie kontrolującemu prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych. Regulacja w tym zakresie obowiązuje również na gruncie obowiązującej Ustawy. Orzekanie w tych sprawach następowało będzie w trybie przepisów Kodeksu postępowania w sprawach o wykroczenia. Sankcją jest kara grzywny. Uznano te działania za czyn mniejszej wagi niż działania opisane w art. 91 projektu. Przepis ten penalizuje przetwarzanie pewnych szczególnych kategorii danych (z art. 9 Rozporządzenia) bez podstawy prawnej. Mając na względzie dobro podmiotów danych oraz wagę naruszenia, jakim jest przetwarzanie danych dotyczących, np. zdrowia, czy seksualności, uznano, że przetwarzanie ich bez podstawy prawnej, a więc nieuprawnione przetwarzanie, powinno być zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku. Tak więc orzekanie w tych sprawach będzie odbywało się w trybie przepisów Kodeksu postępowania karnego.

Należy jednocześnie zwrócić uwagę, iż naruszenie przepisów o ochronie danych może stanowić czyn realizujący znamiona określone w przepisach kodeksu karnego np. w ramach rozdziału XXXIII „Przestępstwa przeciwko ochronie informacji".

W art. 91 projektu ustawy zawarto regułę wydatkową zgodnie z art. 50 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Wskazane kwoty zostały oparte na zawartych w dołączonej do projektu ocenie skutków regulacji i wskazują one różnice w wydatkach budżetu państwa w stosunku do kwot zaplanowanych w ustawie budżetowej.

Ustawa wejdzie w życie w terminie wskazanym w ustawie – Przepisy wprowadzające ustawę o finansach publicznych.

Projekt ustawy będzie miał wpływ na sytuację małych i średnich przedsiębiorców. Należy w tym zakresie wskazać na przyznane Prezesowi Urzędu uprawnienie do wydawania rekomendacji w obszarze zasad zabezpieczania danych osobowych, wypracowywanych z przedsiębiorcami w tym należących do małych i średnich przedsiębiorstw. Zgodnie z treścią projektu, monitorowaniem przestrzegania zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 Rozporządzenia, zajmuje się podmiot akredytowany przez Prezesa Urzędu. Podmiotem takim mogą być przedsiębiorcy w tym mali i średni.
Od dnia 25 maja 2018 r. będzie istniała przewidziana Rozporządzeniem możliwość nałożenia na przedsiębiorców administracyjnych kar finansowych za naruszenie przepisów o ochronie danych osobowych w przypadku nałożenia kary przez Prezesa Urzędu. Trudno w tej chwili oszacować skutki takiego przepisu.

Projekt ustawy o ochronie danych osobowych jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projekt nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.