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.

Rozdział 1 Przepisy ogólne. 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 regulacji. Zgodnie z art. 1, ustawa będzie miała zastosowanie do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych.

Państwa członkowskie nie mają kompetencji prawodawczej do określenia relacji pomiędzy Rozporządzeniem a przepisami implementującymi inne akty prawa wtórnego UE w tym dyrektywę 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 jest aktem prawnym zapewniającym skuteczne stosowanie przepisów Rozporządzenia, nie implementuje jednak przepisów wskazanej dyrektywy, odnosząc się do niej w swojej treści wyłącznie w niewielkim stopniu.

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." W ocenie projektodawcy, pojęcie „osoby prawnej" powinno być intepretowane w świetle legislacji krajowej, obejmując również swoim zakresem tzw. ułomne osoby prawne. Pojęcie danych o firmie i formie prawnej oraz danych kontaktowych powinno obejmować dane konieczne do oznaczania osoby prawnej w obrocie gospodarczym, przy czym nie jest możliwym uznanie, że są to wszystkie dane zawarte przykładowo w Krajowym Rejestrze Sądowym. W ocenie projektodawcy nie powinny być to dane, które przykładowo wskazują na rozdzielność majątkową członka zarządu spółki. 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. Poza organami i instytucjami powoływanymi na podstawie Rozporządzenia, adresatami wynikających z niego obowiązków są z kolei administratorzy, podmioty przetwarzające.

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 podejmo-

wanych 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.

Projektodawca nie zdecydował się wprowadzić do projektu przepisów, określających zakres zastosowania przepisów o ochronie danych osobowych dla bezpieczeństwa narodowego państwa. W polskiej legislacji brak jest bowiem zamkniętego katalogu działań, uznanych za wchodzące w zakres „bezpieczeństwa narodowego". W ocenie projektodawcy decyzja o tym, czy dane działanie uznane powinno być za objęte „bezpieczeństwem narodowym" podjęta powinna być po wnikliwej ocenie każdego stanu faktycznego przez administratora oraz podmiot przetwarzający. Przy czym nie powinno się stosować w tym przypadku wykładni zawężającej ochronę prawa podstawowego jakim jest ochrona danych osobowych. Decyzja taka będzie w dalszej kolejności podlegała działaniom kontrolnym Prezesa Urzędu oraz wymiaru sprawiedliwości. Projektodawca nie zdecydował się również przesądzić relacji zachodzących pomiędzy art. 2 ust. 2 lit. a Rozporządzenia oraz art. 23 ust. 1 lit. a Rozporządzenia w kontekście możliwego użycia w nich tej samej klauzuli „bezpieczeństwa narodowego". TSUE w wyroku Bodil Lindqvist C 101/01 (Wyrok TSUE z 6.11.2003 w sprawie C-101/01, Lindqvist, EU:C:2003:596) wskazał, że „rodzaje działalności wymienione tytułem przykładu w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 (a mianowicie rodzaje działalności, o których stanowią tytuły V i VI Traktatu o Unii Europejskiej, jak również przetwarzanie w ramach działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa oraz w ramach działalności państwa w obszarach prawa karnego) stanowią w każdym razie działania właściwe państwom i władzom państwowym, obce dziedzinom działalności jednostek." W ocenie projektodawcy, odmiennie będzie traktowana sytuacja w obrębie art. 23 Rozporządzenia, ponieważ w tym wypadku bezpieczeństwo narodowe jest jedynie środkiem służącym temu bezpieczeństwu, a nie celem samym w sobie. Innymi słowy istota działalności podmiotu, który będzie korzystał z ograniczenia z art. 23 Rozporządzenia nie będzie ukierunkowana bezpośrednio na bezpieczeństwo narodowe, lecz na inne obszary działalności podlegające prawodawstwu unijnemu. Zakresy art. 2 ust. 2 lit. a , w zw. z art. 4 ust. 2 TUE i art. 23 ust. 1

Rozporządzenia nie pokrywają się, pomimo użycia tej samej klauzuli „bezpieczeństwa narodowego”.

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;

- ograniczenie stosowania Rozporządzenia dla małych i średnich przedsiębiorców.

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. 85 Rozporządzenia przewiduje możliwość ograniczenia przepisów odnoszących się do ochrony danych osobowych, jedynie gdy jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji. Ocena taka podjęta została na etapie tworzenia projektu.

W pierwszej kolejności należy wskazać, że ustawodawca unijny w przepisach rozporządzenia 2016/679 wprowadza dwa rodzaje testów, których przeprowadzenie warunkuje możliwość skorzystania przez państwa członkowskie z ograniczeń w stosowaniu rozporządzenia 2016/679 w określonych celach. Pierwszym z nich, jest przewidziany w art. 23 rozporządzenia 2016/679 test „niezbędności i proporcjonalności", a drugim jest przewidziany chociażby w art. 85 rozporządzenia tekst „niezbędności". O ile jak zostało to wskazane w art. 23 rozporządzenia i odnoszącym się do niego motywie 73 preambuły do rozporządzenia 2016/679 „w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz praw (…) o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym", wymogu proporcjonalności nie przewiduje już ustawodawca unijny w art. 85 rozporządzenia. Zgodnie z odnoszącym się do art. 85 motywem 153 preambuły do rozporządzenia 2016/679 „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". Powołanie się na art. 85 rozporządzenia 2016/679 i skorzystanie z przewidzianej w nim swobody regulacyjnej państwa członkowskiego nie wymaga dokonania więc oceny proporcjonalności proponowanych ograniczeń, a jedynie ich niezbędność. Dodatkowo należy wskazać, że ustawodawca unijny w art. 85 nie wskazuje konkretnych przepisów podlegających możliwemu ograniczeniu, jak zrobił to w art. 23, wskazując jedynie rozdziały. Tym samym ustawodawca unijny przyznał w art. 85 bardzo szeroki zakres swobody regulacyjnej państwom członkowskich, dostrzegając szczególną wartość działań dziennikarskich oraz artystycznych i akademickich. Dokonując wykładni testu niezbędności, Trybunał Konstytucyjny w wyroku z 5 lutego 2008 r. sygn. akt. K 34/06 wskazał, że nakłada on na ustawodawcę „wymóg stwierdzenia rzeczywistej potrzeby dokonania w danym stanie faktycznym ingerencji w zakres prawa bądź wolności jednostki. Z drugiej zaś, winna ona być rozumiana jako wymóg stosowania takich środków prawnych, które będą skuteczne, a więc rzeczywiście służące realizacji zamierzonych przez prawodawcę celów. Ponadto chodzi tu o środki niezbędne, w tym sensie, że chronić będą określone wartości w sposób, bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków. Niezbędność to również skorzystanie ze środków jak najmniej uciążliwych dla podmiotów, których prawa lub wolności ulegną ograniczeniu". W ocenie projektodawcy każde z projektowanych

ograniczeń w obszarze działalności literackiej, działalności artystycznej, wypowiedzi akademickiej oraz działaniach związanych z tworzeniem materiałów prasowych spełnia powyższe wymogi. W szczególności brak wyłączenia przewidzianego w art. 13 rozporządzenia 2016/679 obowiązku informowania osoby, której dane dotyczą o danych pozyskanych od tej osoby w ramach wypowiedzi akademickiej, wyłączyłby w zasadzie możliwość prowadzenia działań dydaktycznych na uczelniach wyższych, wykładach otwartych dla wolnych słuchaczy itd. Prowadzący takie zajęcia nie mógłby dla celów związanych z prowadzonym wykładem zebrać danych uczestników wykładu, bez konieczności zrealizowania wobec nich długiego obowiązku co często przekroczyłoby czas przeznaczony na sam wykład. Jednocześnie forma wypowiedzi akademickiej sama w sobie przesądza, że osoby takie znają cel i dane osoby pozyskującej dane. Z kolei brak wyłączenia prawa do wystąpienia z żądaniem ograniczenia przetwarzania na wniosek osoby, której dane dotyczą mogłoby w ocenie projektodawcy skutkować niemożnością opublikowania wyników badań naukowych. Wypowiedzią akademicką jest bowiem również działalność polegająca na publikowaniu materiałów naukowych na uczelni wyższej. Zrealizowanie skuteczne prawa do ograniczenia danych prowadziłoby do zniekształcenia źródeł będących podstawą stawianych w ramach wypowiedzi akademickiej tez badawczych.

W przypadku działalności podlegającej na tworzeniu materiałów prasowych oraz działalności artystycznej i literackiej wyłączono w szczególności zastosowanie prawa dostępu do danych osobowych. W ocenie projektodawcy w wielu przypadkach uzyskanie takiego prawa mogłoby wiązać się z ujawnieniem tajemnicy dziennikarskiej, wpływając również na proces tworzenia materiałów prasowych oraz proces twórczy. Ciężko sobie bowiem wyobrazić sytuację, w której twórca spektaklu lub dziennikarz miałby pracować pod presją tego, że przed opublikowaniem materiału prasowego lub premierą sztuki ktoś udostępni opracowywane przez nich treści uzyskując dostęp do danych. Ograniczono również zastosowanie obowiązku podawania informacji w przypadku pozyskiwania danych nie od osoby, której dane dotyczą co w ocenie projektodawcy mogłoby wpłynąć chociażby na ograniczenie tajemnicy dziennikarskiej. Obowiązek przekazania informacji o źródle pozyskanych danych mógłby w ogromnym stopniu wpłynąć na działanie polskiej prasy, wpływając również na subiektywizm publikowanych treści. Projektodawca proponuje również wyłączenie prawa do sprostowania danych, co mogłoby skutkować zafałszowaniem procesu twórczego a w przypadku działalności

dziennikarskiej szczególne uprawnienie w tym zakresie przysługuje na podstawie właściwych przepisów sektorowych.

Art. 85 Rozporządzenia nie zawiera wymogu wskazania w treści przepisów wprowadzających odstępstwa (od ogólnych wymogów), iż są one realizowane w celu pogodzenia prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji. Wprowadzenie takiego zastrzeżenia w praktyce w dużej mierze ograniczyłoby możliwość stosowania wyłączenia ze względu na praktyczne problemy z wykładnią niedookreślonych zwrotów: prawa do ochrony danych osobowych oraz wolności wypowiedzi i informacji. Zgodnie z treścią art. 85 Rozporządzenia, Państwa Członkowskie na etapie legislacyjnym mogą wyważyć wskazane w tym przepisie wartości i na tej podstawie wyłączyć lub ograniczyć powołane tam obowiązki i prawa związane z ochroną danych osobowych.

Przepis zakłada skorzystanie przez polskiego ustawodawcę z możliwości ograniczenia stosowania części obowiązków informacyjnych, która została przewidziana w art. 23 Rozporządzenia. Na jego podstawie państwa członkowskie mogą wprowadzić wyłączenia w stosunku do ściśle wymienionych obowiązków i praw, jeśli nie spowoduje to naruszenia istotny podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niebędnym i proporcjonalnym służącym jednemu z wymienionych celów. Rozporządzenie wskazuje, że ingerencja państwa członkowskiego musi służyć jednej z wymienionych przesłanek, m.in. bezpieczeństwu narodowemu, obronie, bezpieczeństwu publicznemu czy „innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego”.

Zgodnie z Rozporządzeniem ograniczenie może dotyczyć takich praw i obowiązków, jak np. obowiązek podawania wskazanych informacji podczas zbierania danych osobowych od osoby, prawo dostępu do danych przysługujących osobie, której dane dotyczą, prawo do sprostowania danych, „prawo do bycia zapomnianym”, prawo do ograniczenia przetwarzania czy prawa do przenoszenia danych.

Projektodawca zdecydował się również ograniczyć zastosowanie rozporządzenia 2016/679 do badań naukowych. Proponowany zapis ma na celu utrzymanie, w granicach dozwolonych rozporządzeniem 2016/679, standardu ochrony danych osobowych w odniesieniu do badań

naukowych tak, jak to jest na gruncie obecnie obowiązujących przepisów. Nadmienić należy, że wyczerpuje on również warunek wskazany w art. 89 ust. 2 rozporządzenia 2016/679, jak również jest zgodny z art. 9 ust. 2 pkt j) ww. dokumentu.

Rozporządzenie 2016/679 dopuszcza zatem możliwość ograniczenia praw związanych z ochroną danych osobowych, jeśli miałoby to umożliwić prowadzenie działalności badawczej i jest podyktowane interesem publicznym. Warunkiem jest, aby cele działalności naukowej, w ramach których dane osobowe są przetwarzane, nie naruszały istoty prawa do ochrony danych i przewidywały odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Należy również zaznaczyć, że proponowany przepis nie ma charakteru bezwzględnego, co oznacza, że skorzystanie z ograniczeń uzasadnione byłoby tylko w ściśle określonych przypadkach. Warto również przywołać zasady określone w motywie 19 preambuły, zgodnie z którą: „(…) państwa członkowskie powinny mieć możliwość zachowania lub wprowadzenia przepisów szczególnych dostosowujących stosowanie przepisów niniejszego rozporządzenia. W takich przepisach możliwe jest doprecyzowanie szczególnych wymogów przetwarzania danych przez te właściwe organy do tych innych celów, z uwzględnieniem konstytucyjnych, organizacyjnych i administracyjnych struktur danego państwa członkowskiego.” Wolność badań naukowych zagwarantowana jest zarówno na gruncie międzynarodowym (art. 13 Karty Praw Podstawowych UE), jak również krajowym (art. 73 Konstytucji RP). Projektowane przepisy służą zabezpieczeniu również prawa wolności badawczej.

Propozycja MNiSW, dotycząca ograniczenia stosowania na gruncie badań naukowych artykułów: 15 (Prawo dostępu), 16 (Prawo do sprostowania), 18 (Prawo do ograniczenia przetwarzania) i 21 (Prawo do sprzeciwu) rozporządzenia 2016/679, wynika z wyraźnego kontrastu, jaki powstał pomiędzy zasadami ogólnymi oraz ustawodawstwem krajowym gwarantującym dotychczas wolność badań naukowych i autonomię uczelni, a regulacjami zawartymi w rozporządzeniu.

Należy jednocześnie wskazać, że wprowadzenie powyższych ograniczeń jest w ocenie projektodawcy konieczne a ich niewprowadzenie uniemożliwi lub poważnie utrudni realizację celów badawczych, a wyjątki takie są konieczne do realizacji tych celów. W szczególności skuteczne zrealizowanie prawa do ograniczenia danych lub sprzeciwu danych mogłoby skutko-

wać usunięciem źródeł będących podstawą stawianych tez badawczych, wpływając na zafałszowanie wyników prowadzonych badań.

Nadmienić należy, że zgodnie z motywem 39 preambuły do rozporządzenia 2016/679, dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Udostępnienie danych osobowych, w tym do celów badań naukowych warunkowane jest wykazaniem słusznego interesu publicznego. Zatem, przyjąć należy, że proponowany zapis ustawy dotyczący ograniczenia stosowania art. 15, art. 16, art. 18 i art. 21 w odniesieniu do badań naukowych, nie spowoduje negatywnych skutków w praktyce.

Szereg badań naukowych prowadzonych m.in. poprzez przetwarzanie danych osobowych, dotyczy wielu dziedzin życia społecznego, w tym z obszaru socjologii, edukacji czy zdrowia publicznego i ma charakter systemowy. Znaczna większość badań systemowych służących identyfikacji i zrozumieniu zjawisk społecznych opierana jest na analizie ściśle określonej grupy lub populacji. Prowadzenie działalności naukowej wymusza korzystanie z różnych źródeł i nie zawsze jest tak, że wiedzy dostarczą dane o charakterze statystycznym. Dostęp do rejestrów i dokumentacji źródłowej jest częstokroć jedyną metodą osiągnięcia założonego celu badawczego. Niemniej, w myśl obowiązującego dotychczas stanu prawnego, standardem jest, że dane osobowe przetwarzane do celów badań naukowych są adekwatne, stosowne i ograniczone do tego, co jest niezbędne dla celów, dla których są przetwarzane. Standardem również jest, że dane osobowe, które służyły działalności badawczej, przechowywane są jedynie w okresie niezbędnego minimum.

Należy również dodać, że zgodnie z art. 4c ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (Dz. U. z 2018 r., poz. 87), Minister prowadzi System Informacji o Nauce w ramach Zintegrowanego Systemu Informacji o Nauce i Szkolnictwie Wyższym „POL-on". W Systemie tym publikowane są wszelkie informacje o działalności naukowej, badawczej i dokonanych osiągnięciach. Dostęp do wielu aspektów związanych z nauką, w tym wyników badań naukowych w Systemie ma na celu m.in. wiarygodną ocenę potencjału naukowego i racjonalne gospodarowanie środkami na naukę i szkolnictwo wyższe, jak również dostarczanie obiektywnych informacji o nauce i szkolnictwie wyższym studentom, kandydatom na studia, pracownikom nauki i przedsiębiorcom. Zaznaczyć należy, że dostęp do wielu informacji, w tym zawierających dane osobowe przetworzone w związku z prowadzoną działalnością nau-

kowo-badawczą, znajdujących się w Zintegrowanym Systemie, jest powszechny. Warto również dodać, że dane zawarte w Systemie mogą być również objęte działalnością badawczą. Rozwiązania przyjęte w rozporządzeniu 2016/679 w zakresie swobodnego prawa do żądania skorzystania z praw wymienionych w art. 15, art. 16, art. 18 i art. 21 rozporządzenia spowodowałoby niekorzystne konsekwencje dla systemu nauki.

Wobec wskazanego powyżej zakresu dozwolonych wyłączeń, projektodawca zdecydował się na odrębne uregulowanie części wymogów w stosunku do szczególnej grupy podmiotów, jaką stanowią przedsiębiorcy z kategorii mikro-przedsiębiorcy. Celem takiej regulacji jest chęć ochrony ważnego interesu gospodarczego w postaci wspierania mikroprzedsiębiorstw.

Rola, jaką podmioty mikroprzedsiębiorcy pełnią w polskiej gospodarce, przyczyniając się do jej wzrostu, jest niekwestionowana. Przejawem ochrony powyższego interesu gospodarczego jest między innymi zagwarantowanie przez ustawodawcę ich szczególnej ochrony w Ustawie o swobodzie działalności gospodarczej. Zgodnie z jej art. 8 „Organy administracji publicznej wspierają rozwój przedsiębiorczości, tworząc korzystne warunki do podejmowania i wykonywania działalności gospodarczej, w szczególności wspierają mikroprzedsiębiorców oraz małych i średnich przedsiębiorców". Wsparcie tych przedsiębiorców będzie też zagwarantowane przez powołanie szczególnej instytucji do ochrony ich praw – Rzecznika Małych i Średnich Przedsiębiorców (zgodnie z przyjętą przez Sejm 26 stycznia 2018 r. ustawą Prawo przedsiębiorców). Co więcej, uwzględnianie preferencji dla mikroprzedsiębiorców nie jest jedynie domeną wąsko pojętego prawa gospodarczego. Również przepisy prawa podatkowego uznają ich szczególną rolę i przewidują pewne ułatwienia (np. w postaci instytucji małego podatnika). Co więcej, prawo unijne również uznaje szczególną rolęmikroprzedsiębiorców. W 2000 r. Rada Europejska przyjęła Europejską Kartę Małych Przedsiębiorstw (Polska podpisała ją w 2002 r.), która stanowi, że „małe przedsiębiorstwa są podstawą gospodarki europejskiej", jednocześnie „jako pierwsze odczuwają negatywne skutki obciążenia nadmierną biurokracją". W związku z powyższym sygnatariusze Karty zobowiązali się do takiego tworzenia otoczenia regulacyjnego, podatkowego i administracyjnego, które będzie sprzyjało działalności mikroprzedsiębiorców. Jednym ze wskazanych w tym dokumencie kierunków wsparcia przez Państwo jest dbanie o dobrą legislację, a jako rekomendowane działanie w tym obszarze wskazano zwolnienie małych przedsiębiorstw z niektórych obowiązków prawnych.

Takie podejście zostało potwierdzone również w innym przyjętym przez Polskę dokumencie – Small Business Act dla Europy (SBA). Stanowi on wyraz zasady „think small first", zgodnie z którą wpływ regulacji na przedsiębiorców należących również do kategorii mikroprzedsiębiorstw powinien być brany pod uwagę na możliwie najwcześniejszym etapie tworzenia nowych regulacji. Celem SBA jest w szczególności trwałe wpisanie zasady „najpierw mikro, małe i średnie przedsiębiorstwa" w kształtowanie polityki począwszy od opracowywania przepisów. SBA jest uznaniem kluczowej roli małych i średnich przedsiębiorstw w gospodarce oraz wprowadzeniem wytycznych (zasad), którymi ustawodawcy unijny i krajowi powinni kierować się przy opracowywaniu i realizacji polityki na szczeblu wspólnotowym oraz krajowym, a także przy formułowaniu konkretnych propozycji legislacyjnych. Do wytycznych (zasad) tych należy w szczególności tworzenie warunków, w których przedsiębiorcy i przedsiębiorstwa rodzinne mogą dobrze prosperować, a przedsiębiorczość jest nagradzana; opracowywanie przepisów zgodnie z zasadą „najpierw mikro, małe i średnie przedsiębiorstwa"; sprawienie, by organy administracji publicznej lepiej reagowały na potrzeby mikroprzedsiębiorstw.

SBA wyraźnie wskazuje też, że obowiązki administracyjne MŚP w tym mikroprzedsiębiorstw w stosunku do dużych przedsiębiorstw są nieproporcjonalnie wysokie. W związku z tym Komisja Europejska wezwała Państwa Członkowskie do „wykorzystania szczególnych środków dla małych i mikro-przedsiębiorstw, takich jak odstępstwa, okresy przejściowe i zwolnienia (szczególnie w zakresie wymogów informacyjnych lub dotyczących sprawozdawczości), a także stosowanie innych środków dopasowanych do specyficznych potrzeb MŚP w odpowiednich przypadkach.". Komisja zobowiązała również Państwa do „korzystania z przepisów dotyczących elastyczności w odniesieniu do MŚP przy wdrażaniu prawodawstwa unijnego oraz unikania nadmiernej regulacji (tzw. „gold-plating")".

Powyższe zasady znalazły swój wyraz również w odniesieniu do Rozporządzenia, a unijny ustawodawca przewidział rozwiązania ułatwiające jego stosowanie do małych przedsiębiorców. Zgodnie z motywem 13 preambuły do Rozporządzenia, „z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw niniejsze rozporządzenie przewiduje wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników". Podobnie w motywie 167 preambuły, wyraźnie wskazuje, że „aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze, tak jak to przewiduje niniejsze rozporządzenie.

Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011. W tym kontekście Komisja powinna rozważyć wprowadzenie szczególnych środków dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw". Za wyraz takiego podejścia może być uznany, zdaniem projektodawcy, również art. 23, który pozwala na wyłączenie stosowania części obowiązków przewidzianych w RODO ze względu na ważny interes gospodarczy. Chcąc jednak ograniczyć zastosowanie proponowanego wyłączenie do jak najmniejszego kręgu osób, projektodawca proponuje określenie kręgu podmiotów uprawnionych do skorzystania z ograniczenia niektórych obowiązków poprzez odwołanie się do unijnej definicją mikroprzedsiębiorców (wskazanej w Załączniku I do rozporządzenia Komisji (UE) nr 651/2014). Zgodnie z tą definicją:

Do grupy obowiązków, z których – zdaniem projektodawcy – celowe jest zwolnienie mikroprzedsiębiorców należą: obowiązek podania niektórych informacji podaczas zbierania danych, m.in. okresu przechowywania danych czy prawa wniesienia skargi do organu nadzorczego, obowiązku dostarczania kopii danych osobowych podlegających przetwarzaniu, obowiązku poinformowania o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania.

Mając na uwadze, że istnieją podmioty, których działalność polega głównie, bądź w znacznym stopniu na przetwarzaniu danych osobowych, projektodawca postanowił wprowadzić istotne ograniczenia w korzystaniu ze zwolnienia.

Przede wszystkim pełny zakres obowiązków informacyjnych będzie dotyczył nawet najmniejszych przedsiębiorców, którzy przetwarzają szczególne kategorie danych wskazane w art. 9 ust. 1 Rozporządzenia (a więc dane ujawniające pochodzenie rasowe lut etniczne, poglądy polityczne, przekonania religijne czy dane biometryczne bądź genetyczne). Nie podlega bowiem żadnym wątpliwościom, że w przypadku przetwarzania tzw. danych wrażliwych niezbędne jest zachowanie restrykcyjnych wymogów i najwyższego standardu ich ochrony przed ich bezprawnym przetwarzaniem.

Druga, odrębna przesłanka wykluczająca możliwość skorzystania ze zwolnienia dotyczy sytuacji, gdy przedsiębiorca udostępnia dane osobowe innym administratorom (chyba że osoba, której dane dotyczą wyraziła na to zgodę lub udostępnienie jest niezbędne do wypełnienia obowiązku ciążącego na administratorze). Celem tego ograniczenia jest wykluczenie z prefe-

rencyjnych przepisów podmiotów, które zajmują się gromadzeniem danych w celu ich dalszego przekazywania (tzw. handlarzy danymi osobowymi). Należy jasno podkreślić, że w takim przypadku zarówno podmiot, który pobierze dane z zamiarem udzielenia ich innemu administratorowi, jak i administrator, który je otrzymał będą objęci wszystkimi wymogami informacyjnymi wskazanymi w Rozporządzeniu. Wyjątki w tym przypadku będą dozwolone jedynie, gdy właściciel danych udzieli zgody na takie udostępnienie (np. w celu otrzymania jakichś korzyści od przedsiębiorcy czy w ramach zgody na ich przekazanie podwykonawcy) lub administrator będzie obowiązany do przekazania danych (np. organom ścigania przestępstw).

Powyższe wyłączenia stosowania wybranych obowiązków informacyjnych nie naruszają istoty podstawowych praw i wolności, jak również są środkiem niezbędnym i proporcjonalnym służącym wyżej opisanemu ważnemu interesowi gospodarczemu Unii oraz państwa członkowskiego.

Przede wszystkim, wskazanym w Rozporządzeniu warunkiem wprowadzenia ograniczeń jest zagwarantowanie, że nie będzie ono naruszało istoty podstawowych praw i wolności. W tym miejscu zasadne wydaje się podkreślenie, że projektowane przepisy nie ingerują w istotę praw osób fizycznych uregulowanych w RODO, czyli w uprawnienie do żądania dostępu, sprostowania czy usunięcia danych gromadzonych przez przedsiębiorcę. Projekt ogranicza się tylko i wyłącznie do złagodzenia stosowania niektórych przepisów dotyczących części obowiązków informacyjnych spoczywających na mikroprzedsiębiorcach. Wyłączenia przewidziane w projektowanychprzepisach w niczym nie uchybiają więc prawom osób, których dane są przetwarzane, a jedynie w pewnym stopniu zmniejszają obciążenia administracyjne spoczywające na przedsiębiorcach.

W szczególności, żadnym ograniczeniom nie będzie podlegał art. 15 ust. 1 i 2 Rozporządzenia, który reguluje zasady prawa dostępu osoby do dotyczących jej danych. Oznacza to, że mimo zwolnienia przedsiębiorcy mikroprzedsiębiorstw z uprzedniego obowiązku poinformowania np. jak długo będzie przechowywał dane, osoba fizyczna w każdej chwili będzie mogła zażądać od przedsiębiorcy uzyskania takiej informacji. W taki sam sposób uzyska informacje o możliwości żądania usunięcia czy sprostowania danych, o możliwości wniesienia skargi do organu nadzorczego czy o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu. Projekt ustawy dopuszcza zwolnienie z konieczności dostarczenia kopii danych

osobowych podlegających przetwarzaniu, jednocześnie przepis art. 15 ust. 1 stanowi, że osoba ma prawo uzyskania dostępu do danych jej dotyczących. Oznacza to, że na przedsiębiorcy będzie ciążył obowiązek zapewnienia takiego dostępu. Niewykluczone, że dla przedsiębiorcy sprzedającego swoje towary bądź usługi „na odległość" jedyną możliwością wywiązania się z tego wymogu będzie dostarczenie osobie fizycznej kopii tych danych. Z kolei planowane ograniczenie stosowania art. 19 zakłada obowiązek powiadomienia o sprostowaniu, usunięciu danych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe. Niemniej w tym kontekście przypomnienia wymaga fakt, że przekazywanie danych osobowych podmiotom trzecim stanowi przesłankę wykluczającą możliwość korzystania z omawianych zwolnień. Do przekazania danych może co prawda dojść również na podstawie zgody osoby, jednak wówczas zastosowanie znajdzie art. 14 Rozporządzenia, który autonomicznie reguluje zasady powiadamiania osoby o posiadaniu jej danych przez podmioty, które weszły w ich posiadanie w inny sposób niż bezpośrednio od niej.

Kolejnym, wskazanym w Rozporządzeniu warunkiem wprowadzenia ograniczeń jest wykazanie, że są one niezbędne i proporcjonalne w demokratycznym społeczeństwie. Warto tę część uzasadnienia rozpocząć od przypomnienia, że zgodnie z utrwalonym orzecznictwem Trybunału zasada proporcjonalności wymaga, aby akty prawne instytucji Unii były odpowiednie do realizacji zgodnych z prawem celów zamierzonych przez dane uregulowanie i nie wykraczały poza to, co konieczne do realizacji tych celów. Przy czym tam, gdzie istnieje możliwość wyboru spośród większej liczby odpowiednich rozwiązań, należy stosować najmniej dotkliwe, a wynikające z tego niedogodności nie mogą być nadmierne w stosunku do zamierzonych celów. Prawodawca ma przy tym szeroki zakres uznania w dziedzinach wymagających od niego dokonywania rozstrzygnięć o charakterze politycznym, gospodarczym i społecznym, a także – dokonywania złożonych ocen. W związku z tym nie chodzi o stwierdzenie, czy środek przyjęty w danej dziedzinie był jedynym możliwym lub najlepszym z możliwych; jedynie oczywiście niewłaściwy charakter tego środka w stosunku do zamierzonego przez właściwe instytucje celu może powodować jego nieważność[1]. Zasada proporcjonalności musi być respektowana także przez organy publiczne, które są zobowiązane do podejmowania wyłącznie niezbędnych działań do osiągnięcia celu, jeśli mogą one negatywnie wpływać na pozycję podmiotu. Takie podejście jest gwarancją zaufania do władz publicznych.

[1] Porównaj: opinia Rzecznika Generalnego TSUE z 6 lipca 2017 r. w sprawie C-304/16.

W związku z powyższym należy podkreślić, że pojęcie „środków koniecznych i proporcjonalnych" na gruncie gospodarczego prawa unijnego to klauzula generalna o bardzo pojemnej treści normatywnej. Uchylana przez RODO dyrektywa 95/46 zezwalała państwom członkowskim na przyjęcie środków ustawodawczych zmierzających do ograniczenia zakresu części praw i obowiązków przewidzianych w tej dyrektywie, jeżeli ograniczenie takie stanowi środek konieczny dla zabezpieczenia ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi. Jednocześnie ocena konieczności takich środków musiała być prowadzona z zapewnieniem poszanowania zasady proporcjonalności[2]. Niezwykle pouczającego przykładu jak w praktyce może wyglądać analiza „konieczności i proporcjonalności" dostarcza unijne prawa rolnego. Zgodnie z art. 40 ust. 2 TFUE stanowi, że wspólna organizacja rynków rolnych może obejmować wszelkie „środki konieczne" do osiągnięcia celów wspólnej polityki rolnej (takich jak np. zwiększenie wydajności rolnictwa przez wspieranie postępu technicznego, racjonalny rozwój produkcji rolnej, jak również optymalne wykorzystanie czynników produkcji, zwłaszcza siły roboczej; albo stabilizacja rynków). W rezultacie, na powyższej podstawie traktatowej, za „konieczne" instrumenty regulacji rynków rolnych uznano między innymi wspólne ceny rolne, system interwencyjnego skupu produktów rolnych, dopłaty z tytułu przechowywania produktów rolnych, różnorodne instrumenty służące limitowaniu produkcji rolnej, dopłaty do konsumpcji produktów rolnych, wsparcie działalności organizacji i zrzeszeń producentów. Do instrumentów regulacji wymiany handlowej z krajami trzecimi należą: refundacje eksportowe, cła, kontyngenty ilościowe, system licencjonowania eksportu i importu produktów rolnych[3]. Oceniając „niezbędność" na gruncie unijnego prawa rolnego ETS ocenił, że o odpowiedzi na pytanie czy dany środek jest konieczny i odpowiedni wymaga bowiem oceny złożonej sytuacji gospodarczej, co oznacza zwyczajowo stosowaną formułę identyfikująca szerokie uprawnienia dyskrecjonalne[4]. Przykład ten dobitnie ilustruje pojemność i elastyczność pojęcia „środków niezbędnych" w prawie unijnym.

W związku z tym analizują zaistnienie przesłanek „konieczności i proporcjonalności" w zakresie ograniczenia części obowiązków informacyjnych dla mikroprzedsiębiorstw na gruncie RODO, podkreślić należy, że – zgodnie z przywołanym powyżej unijnym dokumentem SBA –

[2] Porównaj: wyrok TSUE z 27 września 2017 r., C-73/16.

3 A. Jarosz, Instrumenty regulacji rynków rolnych w uwarunkowaniach wspólnej polityki rolnej UE, Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach, Nr 312, 2017.

[4] Porównaj wyrok ETS w sprawie 5/73, *Balkan-Import-Export*.

gdy duży przedsiębiorca, aby dostosować się do nakładanych regulacji ponosi koszt 1 euro na pracownika, to jednocześnie ten sam obowiązek „kosztuje" przedsiębiorcę już 10 euro na pracownika. Z kolei badania OECD wykazują, że najmniejsze przedsiębiorstwa ponoszą nawet pięciokrotnie wyższe obciążenia administracyjne na pracownika w porównaniu do większych firm[5]. Aby umożliwić funkcjonowanie przedsiębiorcom z tej kategorii konieczne jest zatem stanowienie i implementacja prawa przy uwzględnieniu zasad proporcjonalności. Nadmierne obowiązki prawne, w tym przede wszystkim biurokratyczne, to bowiem jedna z głównych barier dla rozwoju[6]. Tego typu obciążenia przedsiębiorcy traktują jak „ukryte podatki", a ich ciężar najbardziej odczuwa sektor najmniejszych przedsiębiorstw. Jednocześnie ograniczanie nadmiernych obciążeń regulacyjnych, stymuluje rozwój, wspiera konkurencyjność i innowacyjność gospodarki[7]. Dlatego też, dla realizacji ważnego interesu gospodarczego w postaci wspierania mikro-podmiotów niezbędne jest takie ukształtowanie otoczenia prawnego, które uwzględnia ich szczególną wrażliwość na obciążenia administracyjne. Możliwe jest to jedynie wówczas, gdy ustanowione w RODO obowiązki spoczywające na przedsiębiorcach przetwarzających dane osobowe ograniczy się dla mikroprzedsiębiorstw w granicach tam przewidzianych.

Podsumowując powyższą analizę, bez odwołania się przez ustawodawcę krajowego do kompetencji przewidzianej w art. 23, wszystkie obowiązki przewidziane w Rozporządzeniu

spadną w równym stopniu na wszystkich przedsiębiorców, bez względu na ich wielkość, możliwości organizacyjne, doświadczenie czy zakres przetwarzanych danych. Trudno jest byłoby takie rozwiązanie uznać za celowe, konieczne i proporcjonalne. Nie może też budzić żadnych wątpliwości, że w celu dostosowania się do wymogów Rozporządzenia przedsiębiorcy z sektora najmniejszych przedsiębiorstw będą musieli ponieść wysokie koszty (czy to w celu zatrudnienia wyspecjalizowanego pracownika, czy zapewnienia sobie fachowego doradztwa prawnego). Koszty te będą stanowiły dla nich nieproporcjonalnie większe obciążenie aniżeli w przypadku dużych firm, które najczęściej dysponują odpowiednim zapleczem organizacyjnym oraz środkami finansowymi. Z tego powodu projektodawca, proponując zwolnienie z części obowiązków przedsiębiorców z sektora mikroprzedsiębiorstw, ma na uwadze właśnie konieczność takiego wyważenia przepisów, które pozwoli zminimalizować obciążenia nakła-

5 Businesses' Views on Red Tape, Administrative and Regulatory Burdens on Small and Medium-Sized Enterprises, OECD, 2001, str. 41.

6 Bariery prowadzenia działalności gospodarczej w Polsce, 21.06.2017, Związek Przedsiębiorców i Pracodawców, Maison & Partners.

7 The Global Competitiveness Report 2016-2017, World Economic Forum, str. 35.

dane na najmniejsze podmioty, przy jednoczesnym zapewnieniu należytej ochrony właścicielom danych osobowych. W tym konkretnym przypadku jedynie w ten sposób możliwa jest bowiem realizacja ważnego interesu gospodarczego w postaci wspierania mikroprzedsiębiorstw.

Rozdział 2. Inspektorzy ochrony danych. 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. Przepisy projektu w celu zapewnienia stosowania art. 37 ust. 1 lit. a Rozporządzenia precyzują, iż organami i podmiotami publicznymi obowiązanymi do wyznaczenia inspektora są organy publiczne podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

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 zawodo-

wych, 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 Rozporządzenia 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.

Projektodawca nie zdecydował się przewidzieć w projektowanych przepisach instytucji zastępcy inspektora ochrony danych oraz możliwości powołania kilku inspektorów w jednym podmiocie. W opinii projektodawcy, byłoby to niezgodne z Rozporządzeniem. Zgodnie z art. 37 oraz motywem 97 Rozporządzenia administrator i podmiot przetwarzający wyznaczają inspektora, mowa jest o inspektorze w liczbie pojedynczej. Co więcej ustawodawca unijny przewidział możliwość wyznaczenia jednego inspektora dla kilku podmiotów, nie przewidział natomiast możliwości wyznaczenia kilku inspektorów czy tez zastępcy inspektora w jednym podmiocie. Ponadto warto zauważyć, że inspektorem może zostać osoba, która posiada od-

powiednie kwalifikacje zawodowe oraz wiedze fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych, ponadto inspektor ma obowiązek m.in. współpracować z organem nadzorczym oraz pełnić funkcje punktu kontaktowego. Natomiast wyznaczenie zastępców wiąże się z prawem do delegowania uprawnień i obowiązków także w sytuacji gdy w danym podmiocie jest obecny inspektor. Na taką osobę mogłyby zostać przekazane niektóre zadania czy też uprawniania przysługujące inspektorowi. W opinii projektodawcy w przypadku gdy administrator albo podmiot przetwarzający poweźmie wiadomość o długiej nieobecności inspektora ochrony danych osobowych powinien on wyznaczyć nową osobę do pełnienia tej funkcji o czym powinien niezwłocznie zawiadomić Prezesa Urzędu. W przypadku krótszej, okresowej nieobecności administrator bądź podmiot przetwarzający powinien upoważnić innego pracownika do podejmowania działań inspektora.

Rozporządzenie w art. 38 ust. 5 przesądza wprost, że inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. Uwzględniając powyższe, oraz trudności związane z sklasyfikowaniem tajemnicy regulowanej wyłącznie prawem unijnym względem tajemnic regulowanych polskimi przepisami powszechnie obowiązującego prawa, projektodawca zdecydował się nałożyć na inspektorów również w ustawie obowiązek zachowania tajemnicy (tajemnica ustawowa).

Rozdział 3. Akredytacja. 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.

Ministerstwo Cyfryzacji w związku z oceną podjętą w ramach przeprowadzanych konsultacji projektowanych przepisów zdecydowało się zmodyfikować projektowane regulacje w zakresie mechanizmów certyfikacji. Zgodnie z przepisami projektu ustawy o ochronie danych osobowych Prezes Urzędu będzie uprawniony do wydawania certyfikatów, ale do ich wydawania dopuszczeni zostaną również przedsiębiorcy. Celem odciążenia działań podejmowanych przez polski organ nadzorczy, kompetencja do akredytacji podmiotów certyfikujących przyznana będzie z kolei Polskiemu Centrum Akredytacji, będącego krajową jednostką akredytującą w rozumieniu art. 2 pkt 11 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr

765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30). W ocenie projektodawcy powyższe rozwiązania w pełni oddają intencję ustawodawcy unijnego towarzyszącą wprowadzeniu do unijnego porządku prawnego mechanizmu certyfikacji, poprzez włączenie do mechanizmu certyfikacji nie tylko organu nadzorczego ale również innych podmiotów. Z informacji uzyskanych w toku prowadzonych prac legislacyjnych od Komisji Europejskiej wynika, że przyznanie kompetencji do certyfikacji wyłącznie Prezesowi Urzędu budziłoby wątpliwości pod kątem zgodności z art. 42 ust. 5 rozporządzenia 2016/679, który mówi o tym, ze certyfikacji dokonują podmioty certyfikujące lub właściwy organ nadzorczy.

Rozdział 4. Certyfikacja i podmioty certyfikacyjne. Jak zostało to wskazane, zgodnie z przepisami projektu ustawy o ochronie danych osobowych Prezes Urzędu będzie uprawniony do wydawania certyfikatów, ale do ich wydawania dopuszczeni zostaną również przedsiębiorcy. W ocenie projektodawcy jednostka odpowiadająca za certyfikację wewnątrz struktury organizacyjnej Urzędu Ochrony Danych Osobowych powinna posiadać odpowiednią swobodę wewnątrz struktury. Prowadzenie certyfikacji jest odrębnym działaniem niż pozostałe zadania Prezesa Urzędu, w tym zadań związanych z prowadzeniem postępowań w sprawie naruszenia przepisów o ochronie danych, w tym przeprowadzanie czynności kontrolnych.

Przepisy Rozporządzenia nie precyzują dokładnie zakresu możliwej certyfikacji. W szczególności możliwe było uznanie, że certyfikacji mogą podlegać administratorzy oraz podmioty przetwarzające, procesy przetwarzania danych osobowych bądź produkty które w swoim założeniu mają w przyszłości służyć przetwarzaniu danych osobowych. Art. 42 Rozporządzenia wskazuje jedynie, że certyfikaty mają „świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające", nie wskazuje jednak, że ich adresatem mogą być wyłącznie administratorzy bądź podmioty przetwarzające. W świetle powyższego, projektodawca zdecydował się ustanowić szeroki zakres certyfikacji, obejmując nim również administratora, podmiot przetwarzający, producenta albo podmiot wprowadzający produkt na rynek. W ocenie projektodawcy doniosły wymiar certyfikacji w obszarze ochrony danych osobowych uzasadnia przyjęcie jednak jej szerokiego zastosowania, poprzez objęcie mechanizmem certyfikacji nie tylko administratorów i podmiotów przetwarzających, ale również podmioty które produkują rozwiązania słu-

żące przetwarzaniu danych osobowych. Można bowiem wyobrazić sobie ogrom przypadków, w ramach których dany przedsiębiorca nie jest administratorem danych osobowych, ale tworzy systemy informatyczne bądź inne produkty które w przyszłości będą służyły przetwarzaniu takich danych. Rozszerzenie mechanizmów certyfikacji na takie obszary nie tylko nie ogranicza zastosowania przepisów rozporządzenia 2016/679 ale je poszerza, wpływając na podwyższenie poziomu ochrony danych osobowych".

Certyfikacji dokonuje się na wniosek administratora lub podmiotu przetwarzającego. Certyfikacji dokonuje się na podstawie kryteriów określonych przez Prezesa Urzędu bądź podmiot certyfikujący. Jednym z zadań Rady do Spraw Ochrony Danych Osobowych, zwana dalej „Radą". Rada jest organem opiniodawczo-doradczym. Jednym z zadań Rady jest opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych; opiniowanie przekazanych przez Prezesa Urzędu projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych; opracowywanie propozycji kryteriów certyfikacji dla certyfikacji prowadzonej przez Prezesa Urzędu. Pozwoli to na zachowanie dodatkowych warunków bezstronności zasad dokonywania certyfikacji przez Prezesa Urzędu.

Projektodawca zdecydował się uregulować wysokość opłaty pobieranej za czynności certyfikacyjne przez Prezesa Urzędu uznając, że czterokrotność przeciętnego miesięcznego wynagrodzenia za pracę w gospodarce narodowej w roku poprzednim ogłaszanego przez Prezesa Głównego Urzędu Statystycznego, jest opłatą adekwatną. Nie można bowiem zapomnieć, że podmiotami starającymi się o uzyskanie certyfikacji będą wyłącznie podmioty profesjonalne, które fakt certyfikacji będą wykorzystywały w prowadzonej przez siebie działalności, w tym działalności gospodarczej. Projektodawca nie wskazał, na wysokość opłat pobieranych przez podmioty certyfikujące. W ocenie projektodawcy powinny one bowiem pokrywać każdorazowo koszty podejmowane przez przedsiębiorcę certyfikującego oraz będą regulowane przez zasady wolnego rynku z uwzględnieniem elementu konkurencyjności. Projektodawca nie zdecydował się też na uregulowanie wysokości opłaty za akredytację podejmowaną przez Polskie Centrum Akredytacji, determinowanej przez inne przepisy powszechnie obowiązującego prawa, wiążące Polskie Centrum Akredytacji.

W ocenie projektodawcy bardzo ważnym jest, aby podmiot certyfikujący podejmował swoje działania bez narażenia się na konflikt interesów. W szczególności niedopuszczalnym w oce-

nie projektodawcy byłaby sytuacja, w której certyfikacja podejmowana byłaby przez podmiot certyfikujący wobec podmiotów będących w chwili certyfikacji bądź kiedyś klientami podmiotu certyfikującymi w zakresie porad prawnych dotyczących ochrony danych osobowych.

Przepisy art. 25-28 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 5. Kodeksy postępowania. Przepisy rozdziału 5 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. Projektodawca przykłada szczególne znaczenie do możliwej, pełnej transparentności procesu tworzenia kodeksów postępowania. W szczególności zgodnie z motywem 99 preambuły do Rozporządzenia, „sporzą-

dzając kodeks postępowania bądź zmieniając go lub rozszerzając jego zakres, zrzeszenia i inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających powinny konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą, oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji". Projektodawca nie chciał ograniczyć zakresu podmiotów uczestniczących w konsultacjach wyłącznie do określonej kategorii podmiotów jak organizacje społeczne bądź podmioty reprezentujące kategorie administratorów jak izby gospodarcze. W świetle powyższego, projekt nakłada ogólny obowiązek konsultacji tworzonych kodeksów z zainteresowanymi podmiotami.

Rozdział 6. Prezes Urzędu Ochrony Danych Osobowych. Rozdział 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.

Przepisy projektowanej ustawy stawiają zgodnie z wymogami przewidzianymi w rozporządzeniu 2016/679 wysokie wymogi stawiane Prezesowi Urzędu. W szczególności przewiduje, że musi on wyróżniać się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych.

Z uwagi na ogromne doświadczenie w sprawowaniu nadzoru nad ochroną danych osobowych przez Generalnego Inspektora Ochrony Danych Osobowych, założeniem jest zapewnienie faktycznej ciągłości działania organu. W związku z powyższym, z dniem wejścia w życie ustawy pracownicy zatrudnieni w Biurze Generalnego Inspektora Ochrony Danych Osobowych stają się pracownikami Urzędu Ochrony Danych Osobowych, mienie Skarbu Państwa będące we władaniu Generalnego Inspektora Ochrony Danych Osobowych staje się mieniem Prezesa Urzędu Ochrony Danych Osobowych, a należności i zobowiązania Generalnego Inspektora Ochrony Danych Osobowych z dniem wejścia w życie ustawy stają się należnościami i zobowiązaniami Prezesa Urzędu Ochrony Danych Osobowych. Organ będzie organem kadencyjnym, odwołalnym w wyjątkowych, wynikających z rozporządzenia 2016/679 przypadkach. Zgodnie z art. 53 ust. 4 Rozporządzenia „członek organu nadzorczego może zostać odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki niezbędne do pełnienia obowiązków". Celem wzmocnienia niezależności organu nadzorczego, projektodawca zdecydował się wskazać, że odwołanie możliwe jest nie tylko w razie poważnego uchybienia, ale tylko gdy takie uchybienie zostało stwierdzone prawomocnym wyrokiem sądu i polegało na popełnieniu umyślnego przestępstwa lub umyślnego przestępstwa skarbowego. Wzmocnieniu pozycji organu nadzorczego służyć mają również takie projektowane instrumenty jak przyznanie organowi prawa do przeprowadza-

nia niezapowiedzianych kontroli naruszenia zasad ochrony danych osobowych, przeprowadzania kontroli planowanych czy możliwość korzystania z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji w toku przeprowadzanej kontroli. Organ sam będzie również decydował o nadawaniu sobie statutu – obecnie robi to Prezydent Rzeczpospolitej Polskiej. Jednocześnie należy wskazać, że utrzymana zostanie pozycja ustrojowa organu jako podlegającego wyłącznie ustawie, kadencyjnego i nie należącego do administracji rządowej. Projektodawca w związku z przeprowadzonymi konsultacjami społecznymi zdecydował się ostatecznie nie zmieniać w żadnym zakresie procedury powołania organu – względem aktualnie obowiązujących regulacji. Organ zgodnie z projektem będzie więc powoływany przez Sejm Rzeczpospolitej Polskiej za zgodą Senatu Rzeczpospolitej Polskiej. Organ będzie również na etapie jego powoływania składał ślubowanie przed Sejmem Rzeczpospolitej Polskiej, dysponując również immunitetem formalnym. Kandydat na stanowisko Prezesa Urzędu będzie musiał spełnić kryterium wyższego wykształcenia, wiedzy i doświadczenia z zakresu ochrony danych osobowych.

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 Urzędu 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 .

W przypadku odwołania Prezesa Urzędu, uprawnienie do odwołania zastępcy przysługiwało będzie Prezesowi Urzędu a udział ministrów ogranicza się jedynie do wydania swojej opinii w sprawie.

Należy w szczególności wskazać, że wprowadzenie zmian w procedurze powołania Prezesa Urzędu względem procedury obowiązującej obecnie w przypadku Generalnego Inspektora Ochrony Danych Osobowych, ma na celu wzmocnienie niezależności organu. Po pierwsze bowiem, obowiązujące obecnie przepisy prawne przewidują, że odwołania zastępcy może dokonać Marszałek Sejmu na wniosek GIODO. Powyższe oznacza, że Marszałek Sejmu nie jest związany wnioskiem GIODO i może odmówić odwołania Zastępcy GIODO. Projektowana regulacja przewiduje, że odwołania zastępcy Prezesa Urzędu dokonuje Prezes Urzędu bez konieczności podejmowania w tym zakresie jakiejkolwiek konsultacji z innym organem. Po drugie, przepisy wskazują wyraźnie, że to Prezes Urzędu powołuje swoich zastępców a nie tak jak obecnie inny organ państwowy – w obowiązującej ustawie Marszałek Sejmu. Po trzecie wreszcie, Prezes Urzędu nie będzie związany wniosek ministra w przedmiocie powołania zastępców, co wskazuje wprowadzony do ustawy zwrot „może powołać”. Wreszcie po czwarte, w przypadku powołania przez Prezesa Urzędu jakiegokolwiek zastępcy, będzie bardziej swobodny w odwołaniu ich. W świetle obowiązujących obecnie przepisów ustawy, GIODO swobody takiej nie ma.

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. Ideą jest by różne podmioty mogły wesprzeć swoją wiedzą Prezesa Urzędu.

Przepisy projektu stanowią o sprawozdaniach składanych przez Prezesa Urzędu i służy zapewnieniu stosowania art. 59 Rozporządzenia.

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.

Projekt zawiera też 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. Przepisy dotyczą 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.

Projekt 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.

Projekt nakłada na Prezesa Urzędu obowiązek opracowywania i udostępniania rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeń-

stwa 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.

Prezes Urzędu jest organem uprawnionym do prowadzenia dużej liczby postępowań. Dla celów porządkowych należy wskazać, że w przypadku postępowania w sprawach naruszenia przepisów o ochronie danych osobowych, w sprawach nieuregulowanych w ustawie do postępowania przed Prezesem Urzędu stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Do procedury zawiadomienia, zmiany danych i odwołania przez Prezesa Urzędu wyznaczenia przez administratora albo podmiot przetwarzający inspektora ochrony danych osobowych, do procedury akredytacji podmiotów certyfikujących, do certyfikacji oraz do procedury zatwierdzania kodeksów postępowania nie stosuje się przepisów Kodeksu postępowania administracyjnego. **Rozdział 7. Postępowanie w sprawie naruszenia przepisów o ochronie 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 niepropocjonalne. 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 Konstytu-

cyjny 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. Należy wreszcie wskazać, że projektodawca zdecydował się wprowadzić do projektu „jednoinstancyjność" postępowania mimo brzmienia art. 127 a Kodeksu. Zgodnie z treścią rzeczonego artykułu w świetle w trakcie biegu terminu do wniesienia odwołania strona może zrzec się prawa do wniesienia odwołania wobec organu administracji publicznej, który wydał decyzję. W ocenie projektodawcy nawet treść takiego artykułu nie wyeliminowuje przypadków, w których jedna ze stron chociażby celem przedłużenia postępowania, zdecyduje się złożyć odwołanie. Uwzględniając charakter ochrony danych osobowych jako prawa podsta-

wowego, działanie takie w ocenie projektodawcy mogłoby pociągnąć za sobą poważne konsekwencje.

Obok jednoinstancyjności kolejną odrębnością postępowania przewidzianego w ustawie w stosunku do postępowania unormowanego w Kodeksie jest wskazanie, że w sprawach związanych z ochroną danych osobowych pełnomocnikiem może być przedstawiciel organizacji, do której zadań statutowych należą sprawy związane z ochroną danych osobowych. Powyższa regulacja ma na celu zapewnienie stosowania art. 80 Rozporządzenia. Powołany przepis nakłada na państwa członkowskie obowiązek przewidzenia w przepisach prawnych rozwiązania, w świetle którego organizację lub zrzeszenie – które nie ma charakteru zarobkowego i ma cele statutowe leżące w interesie publicznym i działa w dziedzinie ochrony danych osobowych – można umocować do wniesienia w jej imieniu skargi oraz wykonywania w jej imieniu praw. Zgodnie z treścią motywu 142 preambuły do Rozporządzenia, „jeżeli osoba, której dane dotyczą uzna, że naruszane są jej prawa wynikające z niniejszego rozporządzenia, powinna mieć ona prawo zlecić podmiotowi, organizacji lub zrzeszeniu wniesienie skargi w swoim imieniu do organu nadzorczego, wykonanie prawa do środka ochrony prawnej przed sądem w imieniu osób, których dane dotyczą lub – o ile taką możliwość przewiduje prawo państwa członkowskiego – żądanie odszkodowania w imieniu osób, których dane dotyczą". Projektowana regulacja stanowi niezależną podstawę dla działania przedstawiciela organizacji. Przepis nie wyłącza jednocześnie art. 31 Kodeksu, który będzie miał pełne zastosowanie. Wprowadzenie do ustawy ww. przepisu obok art. 31 Kodeksu daje pełną skuteczność stosowania przepisów Rozporządzenia. Należy również wskazać, że podobna regulacja wprowadzona została do art. 87 § 5 ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego (Dz. U. 2018 poz. 155). Zgodnie z treścią powołanego przepisu, w sprawach związanych z ochroną praw konsumentów pełnomocnikiem może być przedstawiciel organizacji, do której zadań statutowych należy ochrona konsumentów. Należy w tym przypadku wskazać, że projektowane przepisy pozostają w pełnej zgodności z przewidzianą w polskim porządku prawnym istotą pełnomocnictwa przypisanego do określonej osoby fizycznej, które w tym przypadku musi być jednak przedstawicielem organizacji. Pełnomocnikiem cały czas pozostanie więc osoba reprezentująca organizację a nie organizacja jako taka.

w projekcie ustawy wprowadzono również rozwiązanie zgodnie z którym Prezes Urzędu zawiadamiając strony o niezałatwieniu sprawy w terminie, obowiązany jest również poinfor-

mować o stanie sprawy i przeprowadzonych w jej toku czynnościach. Należy wskazać, że powołana regulacja uzupełnia art. 36 Kodeksu i służy zapewnieniu pełnego 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 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 powyższa regulacja 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. W ocenie projektodawcy państwo członkowskie wzmacniając ochronę danych osobowych może w praktyce zobowiązać organ nadzorczy do informowania osób których dane dotyczą wcześniej, niż po upływie trzech miesięcy, a okres wynikający z Rozporządzenia jest okresem maksymalnym.

Projektowany przepis art 56 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. W związku z powyższym, zakres dostępu Prezesa Urzędu do informacji ustawowo chronionych będzie determinowany każdorazowo przepisami obejmującymi informacje ochronione. W ocenie projektodawcy z uwagi na możliwe ryzyko wykładni art. 58 Rozporządzenia w związku z art. 90 Rozporządzenia, zgodnie z którą w braku wyraźnej regulacji krajowej organ nadzorczy jest uprawniony do korzystania z uprawnień określonych w art. 58 ust 1 pkt e) i f) Rozporządzenia, tj. uzyskiwania dostępu do danych osobowych i informacji, a także pomieszczeń i urządzeń niezbędnych do realizacji zadań organu nadzorcze-

go, bez względu na obowiązek podmiotu kontrolowanego do zachowania tajemnicy, wynikający z regulacji sektorowych, postanowiono o wprowadzeniu do projektu właściwych przepisów. Z rozporządzenia nie wynika bowiem w sposób wyraźny zakaz korzystania z ww. uprawnień organu nadzorczego w zakresie, w jakim ich realizacja mogłaby być sprzeczna z ochroną tajemnic sektorowych. Na gruncie Rozporządzenia wydaje się, że uprawnienia te nie doznają ograniczeń, a relacja rozporządzenia do krajowych regulacji tajemnic sektorowych może być różnie interpretowana. W ocenie projektodawcy przepis art. 90 Rozporządzenia należy rozumieć w ten sposób, że państwa członkowskie mogą ukształtować uprawnienia organu nadzorczego, o których mowa w art. 58 ust. 1 pkt e) i f) ze względu na tajemnice zawodowe lub inne obowiązki równoważne zachowaniu tajemnicy, jeśli jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy. Państwa członkowskie mogą zatem uprawnienia przysługujące organowi nadzorczemu na podstawie art. 58 ust. 1 pkt e) i f) ograniczyć lub wyłączyć. Taka interpretacja przepisu art. 90 jest w ocenie projektodawcy zgodna z celem tego przepisu i motywem 164, które mają na celu przede wszystkim umożliwienie państwom członkowskim zapewnienia w przepisach krajowych ochrony tajemnic zawodowych. W ocenie projektodawcy proponowane przepisy pozostają w pełnej zgodności z rozporządzeniem 2016/679. Dostęp organu nadzorczego do informacji objętych tajemnicami odbywać się będzie w trybie, w zakresie i na zasadach przewidzianych w przepisach regulujących poszczególne tajemnice. Dane osobowe nie są bowiem wartością absolutną i ich ochrona nie może odbywać się kosztem narażenia na ujawnienie informacji chronionych szczególnymi reżimami. Projektowana ustawa powinna natomiast wyraźnie stanowić, że organ nadzorczy nie jest uprawniony do korzystania z uprawnień określonych w art. 58 ust. 1 pkt e) i f) Rozporządzenia w zakresie, w jakim informacje, które mogłyby zostać ujawnione w toku wykonywania czynności, w ramach postępowania, podlegają ochronie jako tajemnica zawodowa. Ewentualny dostęp organu nadzorczego do informacji objętych tajemnicami sektorowymi powinien się odbywać, w trybie, zakresie i na zasadach przewidzianych w przepisach regulujących poszczególne tajemnice. Dane osobowe nie są bowiem wartością absolutną i ich ochrona nie może odbywać się kosztem narażenia na ujawnienie informacji chronionych szczególnymi reżimami ochronnymi poza szczególnie uzasadnionymi przypadkami.

Przepisy projektu odnoszą się też 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. Projektodawca zdecydował się jednak nałożyć na przedsiębiorców obowiązek dostarczenia Prezesowi Urzędu wersji dokumentu niezawierającą informacji objętych zastrzeżeniem. W przypadku nie dostarczenia wersji dokumentu niezawierającej informacji objętych zastrzeżeniem, zastrzeżenie uważa się za nieskuteczne. Projektowane rozwiązanie ma w swoich istocie wzmocnić potrzebę ochrony informacji objętych tajemnicą przedsiębiorstwa uznając, że to przedsiębiorcy ustanawiający taką tajemnicę najlepiej potrafią ocenić jej zakres w każdym stanie faktycznym. Proponowane przepisy należy również oceniać w świetle przyznanych stronom uprawnień wglądu do akt sprawy, co wiąże się bardzo często z koniecznością usuwania z ich treści informacji objętych takimi tajemnicami, narażając organ na znaczne obciążenia.

Odnosząc się do ograniczenia prawa wglądu do materiału dowodowego 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.

Przepisy stanowi modyfikację przepisu art. 88 Kodeksu. Celem tego przepisu jest zwiększenie 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 wskazanie minimalnej wysokości grzywny na kwotę 500 zł oraz maksymalnej na kwotę 5000 zł uzasadnione jest

wagą spraw związanych z naruszeniem przepisów o ochronie danych osobowych, co wymaga zapewnienia sprawności i skuteczności postępowań w tych sprawach. Należy wskazać, że zgodnie z art. 189b Kodeksu postępowania administracyjnego przez administracyjną karę pieniężną rozumie się określoną w ustawie sankcję o charakterze pieniężnym, nakładaną przez organ administracji publicznej, w drodze decyzji, w następstwie naruszenia prawa polegającego na niedopełnieniu obowiązku albo naruszeniu zakazu ciążącego na osobie fizycznej, osobie prawnej albo jednostce organizacyjnej nieposiadającej osobowości prawnej. Zgodnie zaś z przepisem art. 189a §1. Kodeksu w sprawach nakładania lub wymierzania administracyjnej kary pieniężnej lub udzielania ulg w jej wykonaniu stosuje się przepisy działu Dział IVA. Administracyjne kary pieniężne. Reasumując, w przypadku grzywien przewidzianych w Kodeksie postępowania administracyjnego (art. 88 oraz art. 96) z uwagi na fakt, iż grzywna ww. jest nakładana w drodze postanowienia, nie znajduje zastosowania Dział IVA KPA. Jednakże mając na uwadze obowiązujące w demokratycznym państwie prawnym zasady, w szczególności na zasadę proporcjonalności oraz zasadę zaufania do organów państwa w orzecznictwie i doktrynie postuluje się, aby wprowadzać gwarancje procesowe oraz przesłanki wymiaru sankcji administracyjnej w każdym przypadku wymierzania sankcji pieniężnych. Z uwagi na dużą rozpiętość przewidzianej sankcji pieniężnej (w przeciwieństwie do art. 88 Kodeksu, gdzie maksymalna wysokość grzywny wynosi 200 zł.) w ocenie projektodawcy zasadne jest wprowadzenie przesłanek wymiaru kary grzywny.

Przepisy projektu mają 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. Zdecydowano się wprowadzić do przepisów projektu ustawy instytucję skargi na to postanowienie. Należy wskazać, że wprowadzone przez projektodawcę uprawnienie jest uprawnieniem wykraczającym poza przewidziane w art. 58 rozporządzenia 2016/679. Państwa członkowskie uprawnione są do wprowadzania rozwiązań proceduralnych wykraczających poza przewidziane w rozporządzeniu 2016/679 o ile są one konieczne do zapewnienia jego skutecznego stosowania bądź w żadnym zakresie nie ograniczają pozycji ustrojowej oraz

zadań Prezesa Urzędu zagwarantowanych mu przepisami rozporządzenia 2016/679. Przyznanie Prezesowi Urzędu odrębnego środka prawnego do wydawania postanowień nakazujących czasowe ograniczenie przetwarzania danych w ocenie projektodawcy wzmacnia uprawnienia Prezesa Urzędu a jego wprowadzenie możliwe jest w świetle przysługującej wszystkim państwom członkowskim autonomii proceduralnej. Wprowadzenie tak szczegółowej regulacji wskazującej wymogi które muszą być spełnione by postanowienie takie wydać, uzasadnione jest z kolei charakterem takich postanowień, które mogą mieć ogromny wpływ na działalność gospodarczą. Rozwiązanie wprowadzone do projektu ustawy o ochronie danych osobowych nie jest jednak 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. Wreszcie, jak zostało to już wskazane 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.

W projekcie ustawy – w zakresie rozstrzygnięć jakie mogą zapaść po przeprowadzeniu postępowania nie odesłano do art. 58 ust. 2 lit. b-j Rozporządzenia. Uznano za niecelowe przepisywanie oraz powoływanie się na obowiązujące przepisy Rozporządzenia w tym zakresie, wywołujące przecież bezpośredni skutek, i podlegające bezpośredniemu zastosowaniu. 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.

Zgodnie z projektowanymi przepisami, organy lub podmioty publiczne, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, w stosunku do których Prezes Urzędu wydał prawomocną decyzję stwierdzającą naruszenie, niezwłocznie podają do publicznej wiadomości na swojej stronie internetowej lub stronie podmiotowej Biuletynu Informacji Publicznej, informację o działaniach podjętych w celu wykonania 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 przepisach projektu ograniczono wysokość administracyjnej kary pieniężnej, którą można nałożyć na podmioty publiczne do 100 000 zł. Projektodawca dostrzega bowiem specyfikę sektora publicznego, który powinien zapewniać pełną transparentność swoich działań. Zapewniając pełną transparentność działań Prezesa Urzędu, projektodawca nałożył na organ obowiązek każdorazowej oceny, czy wydawane przez niego decyzje nie powinny w interesie publicznym zostać przez niego udostępnione. Projektodawca odstąpił jednak od nałożenia na Prezesa Urzędu obowiązku publikowania przez niego wszystkich decyzji, kierując się chęcią zapewnienia sprawności działania organu i odciążając go od nadmiernych obowiązków administracyjnych. W przypadku niektórych z wydawanych decyzji z uwagi na ich drobny przedmiot, ich udostępnienia może okazać się niecelowe.

Odnosząc się do projektu wskazać należy, że projektodawca odstąpił od przesądzania, że każda z decyzji wydanych przez Prezesa Urzędu podlega rygorowi natychmiastowej wykonalności. Projektodawca uznał bowiem, że norma taka miałaby charakter informacyjny, a rygor natychmiastowej wykonalności decyzji Prezesa urzędu będzie wynikał z właściwych przepisów powszechnie obowiązującego prawa - co nie wymaga powtarzania w projektowanej ustawie. Należy wyjaśnić, że zgodnie z projektem ustawy postępowanie przed Prezesem Urzędu jest postępowaniem jednoinstancyjnym, a więc od decyzji wydanej przez Prezesa Urzędu nie służy odwołanie (wniosek o ponowne rozpatrzenie sprawy). Konsekwencją wprowadzenia jednoinstancyjnego postępowania jest to, że decyzje wydane przez Prezesa Urzędu są ostateczne i wykonalne z mocy samego prawa. Podlegają one wykonaniu z chwilą doręczenia decyzji stronie. Rygor natychmiastowej wykonalności, zgodnie z art. 108 Kodeksu

może zostać nadany decyzji nieostatecznej a więc takiej od której służy odwołanie w administracyjnym toku instancji, ergo decyzji od której nie służy odwołanie nie nadaje się rygoru natychmiastowej wykonalności ponieważ te decyzje są ostateczne i podlegają natychmiastowemu wykonaniu z chwilą doręczania ich stronie. Usunięcie przez projektodawcę normy wprost przesądzającej o natychmiastowej wykonalności decyzji, nie zmieni to faktu, iż decyzje wydane przez Prezesa Urzędu w postępowaniu jednoinstancyjnym będą podlegały wykonaniu. Projektodawca mając natomiast na uwadze, że zgodnie z Rozporządzeniem kary pieniężne mogą być bardzo dotkliwe dla ukaranych podmiotów, chciał wprowadzić wyjątek od wskazanej powyżej zasady, polegający na tym, że w przypadku wniesienia przez stronę skargi do sądu administracyjnego decyzja w zakresie dotyczącym administracyjnej kary pieniężnej podlega wstrzymaniu wykonania. Warto również zauważyć, że bez projektowanego przepisu strona mogłaby w skardze na decyzję Prezesa Urzędu wystąpić z wnioskiem o wstrzymanie wykonania decyzji w całości lub w części (art. 61 § 3 p.p.p.s.a.), postanowiono jednak wprowadzić wstrzymanie wykonania decyzji w zakresie w którym decyzja dotyczy administracyjnej kary pieniężnej z mocy ustawy bez konieczności składania przez stronę wniosku w tej sprawie. Strona na podstawie rzeczonego artykułu będzie mogła wystąpić z wnioskiem o wstrzymanie wykonania decyzji w pozostałym zakresie.

W projekcie uregulowano w zakresie niezbędnym postępowanie konsultacyjne o którym mowa w art. 36 Rozporządzenia. Ograniczono się do wskazania wymogów formalnych pisma, ze względu na ekonomikę legislacyjne poprzez odpowiednie odesłanie do art. 63 Kodeksu. Ma to na celu możliwość weryfikacji wniosku po przez obowiązek opatrzenia wniosku podpisem, gdyż obowiązek ten nie wynika bezpośrednio z art. 36 Rozporządzenia. Należy jednocześnie pokreślić, że do przeprowadzenia konsultacji nie znajdą zastosowanie przepisy kodeksu postępowania administracyjnego, gdyż nie przeprowadzenie konsultacji nie kończy się decyzją administracyjną ani żadnym innym władczym działaniem organu.

Projekt ma na celu dostosowanie polskiego prawa do wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie Wyrok Trybunału Sprawiedliwości UE w sprawie Maxa Schremsa, stwierdzający nieważność decyzji Komisji Europejskiej zatwierdzającej porozumienie Safe Habor wyrok (C-362/14). W przedmiotowej sprawie TSUE stwierdził, że Komisja Europejska która stwierdza, że państwo trzecie zapewnia odpowiedni stopień ochrony, nie stoi na przeszkodzie temu, aby organ nadzorczy państwa członkowskiego, rozpatrzył skargę danej osoby

związaną z ochroną jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, przekazanych z państwa członkowskiego do tego państwa trzeciego, gdy osoba ta podnosi, że prawo i praktyka obowiązujące w tym państwie trzecim nie zapewniają odpowiedniego stopnia ochrony. Jednocześnie jednak TSUE wskazał jednoznacznie, iż tylko jemu przysługuje prawo do stwierdzenia nieważności takiej decyzji.

W efekcie powstała sytuacja, w której krajowy organ nadzorczy ma kompetencje do rozpatrywania spraw obywateli, których dane są przetwarzanie na podstawie decyzji Komisji Europejskiej, lecz do puki jest ona w porządku prawnym, do póty de facto nie może on realizować w pełni swojej kompetencji. TSUE stwierdził także, że o ile sądy krajowe mają prawo badać ważność aktu unijnego, takiego jak decyzja Komisji, to jednak nie są one właściwe do samodzielnego stwierdzenia nieważności takiego aktu. A fortiori, krajowe organy nadzorcze nie mają prawa samodzielnie stwierdzić nieważności takiej decyzji przy rozpatrywaniu, dotyczącej zgodności decyzji Komisji Europejskiej. Także krajowe sądy taką kompetencją nie dysponują.

W konkluzji TSUE wskazał, że jeżeli organ nadzorczy uzna zarzuty podniesione przez osobę, która wniosła do niego skargę dotyczącą ochrony jej praw i wolności w zakresie przetwarzania danych osobowych, za zasadne, organ ten powinien – mieć prawo pozywania do sądu. W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji.

Mając na uwadze fakt, iż podstawową zasadę ustrojową, iż kontrola administracji publicznej jest dokonywana przez sądy administracyjne projektodawca zdecydował się pozostawić ww. kompetencję sądom administracyjnym. Należy jednak wskazać, że podstawą zasadą działania sądów administracyjnych jest zasada skargowości, czyli badania wydanych przez organy administracji publicznej aktów administracyjnych, które są zaskarżane przez strony postepowania. Ta podstawowa funkcja i model kontroli sądowo administracyjnej wynikającej z art. 1 i art. 2 ustawy – Prawo przed sądami administracyjnych nie znajduje zastosowania ww. przypadku.

W efekcie projektodawca mając na uwadze zdecydował się wprowadzić odrębną procedurę w ustawie o ochronie danych osobowych. Nie jest to jednak procedura oderwana w całości od rozwiązań przewidzianych w kodeksie postępowania administracyjnego oraz ustawy – Prawo o postępowaniu przed sądami administracyjnymi.

Zgodnie z artykułem art. 1 ustawy z dnia z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (dalej ppsa). Ustawa ta normuje postępowanie sądowe w sprawach z zakresu kontroli działalności administracji publicznej oraz w innych sprawach, do których jego przepisy stosuje się z mocy ustaw szczególnych (sprawy sądowoadministracyjne). Prawo do wprowadzenia nowej kompetencji dla sądów administracyjnych, niezwiązanych wyłącznie z „kontrolą administracji publicznej" wynika wprost z art. 1 ww. ustawy. Zgodnie natomiast z art. 63 i art. 64 ppsa jeżeli ustawy tak stanowią, postępowanie sądowe wszczyna się na wniosek. Wniosek składa się bezpośrednio do sądu. Wniosek powinien czynić zadość wymaganiom pisma w postępowaniu sądowym, a ponadto zawierać określenie żądania, jego podstawy i uzasadnienie oraz oznaczenie stron i organów, a także spełniać inne wymagania określone w przepisach szczególnych. Przepis ten stanowi także, że do wniosku stosuje się odpowiednio przepisy o skardze, jeżeli ustawa nie stanowi inaczej. W efekcie w ustawie o ochronie danych osobowych przyjęto następujące rozwiązanie.

Prezes Urzędu podejmując z urzędu lub na wniosek postępowanie w sprawie stwierdzenia naruszenia przepisów o ochronie danych osobowych ustalając, iż przetwarzanie danych osobowych strony postępowania następuje m.in. na podstawie decyzji Komisji Europejskiej oraz uznając iż istnieją uzasadnione wątpliwości, że decyzja Komisji Europejskiej jest niezgodna z prawem Unii Europejskiej, na podstawie art. 97 kodeksu postepowania administracyjnego zawiesza swoje postepowanie. Zgodnie bowiem z art. 97 § pkt 4 Kodeksu organ zawiesza postępowanie, gdy rozpatrzenie sprawy i wydanie decyzji zależy od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd. Jak wskazuje się w literaturze zgodnie z którym przepis art. 97 § 1 pkt 4 Kodeksu nie daje podstaw do tego, aby zawęzić krąg podmiotów kompetentnych do rozstrzygnięcia zagadnienia wstępnego tylko do polskich sądów lub organów. Przemawia bowiem przeciwko temu zarówno wykładnia językowa, jak i systemowa, odwołująca się do koncepcji źródeł prawa powszechnie obowiązującego (W. Chróścielewski). Ponadto jak wskazał WSA w Warszawie SA/Wa 1898/06, Legalis pojęcie sądu, użyte w art. 97 § 1 pkt 4 Kodeksu, musi podlegać wykładni dynamicznej i celowościowej,

uwzględniającej zmiany systemu wymiaru sprawiedliwości (powołanie TK) oraz dopuszczenie jurysdykcji sądów międzynarodowych, takich jak Europejski Trybunał Praw Człowieka oraz Trybunał Sprawiedliwości UE. W niniejszej sytuacji za powyższym w ocenie projektodawcy przemawia fakt, iż sprawa przed TSUE w sprawie ważności decyzji administracyjnej zostanie wszczęta w indywidualnym postępowaniu. Następnie Prezes Urzędu wystąpi na podstawie przepisów ustawy o ochronie danych osobowych do sądu administracyjnego z wnioskiem (będzie to wniosek o którym mowa w art. 63-64 ppsa) o wydanie orzeczenia w sprawie ważności decyzji Komisji Europejskiej. W celu wyjaśnienia, należy wskazać, że zgodnie z ogólną regułą zawartą w art. 13 ppsa sądem właściwym do rozpatrzenia wniosku Prezesa Urzędu będzie wojewódzki sąd administracyjny.

Następnie, z uwagi na wyłączną kompetencję TSEU w zakresie stwierdzenia ważności decyzji Komisji Europejskiej, sąd administracyjny będzie w przypadku przyjęcia wątpliwości Prezesa Urzędu za zasadne wystąpi z zapytaniem prawnym do TSUE. W przeciwnym wypadku sąd administracyjny wyda stosowne postanowienie. W celu zagwarantowania prawa do uczestniczenia w procedurze sądowoadministracyjnej wszystkim stronom postępowania prowadzonego przed Prezesem Urzędu, wskazano w ustawie wprost, iż są one również stronami postępowania sądowoadministracyjnego. Obowiązek wystąpienia przez sąd administracyjny z pytaniem prawnym do TSUE w ocenie projektodawcy będzie wynikał z faktu, iż postepowanie przez sądem administracyjnym będzie miało charakter jednoinstancyjny. Od postanowienia sądu administracyjnego nie będzie przysługiwał środek odwoławczy. Zgodnie natomiast Artykuł 267 Traktatu o Unii Europejskiej i Traktatu o Funkcjonowaniu Unii Europejskiej (2016/C 202/01) Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania w trybie prejudycjalnym: o wykładni Traktatów oraz o ważności i wykładni aktów przyjętych przez instytucje, organy lub jednostki organizacyjne Unii. W przypadku gdy pytanie z tym związane jest podniesione przed sądem jednego z Państw Członkowskich, sąd ten może, jeśli uzna, że decyzja w tej kwestii jest niezbędna do wydania wyroku, zwrócić się do Trybunału z wnioskiem o rozpatrzenie tego pytania. W przypadku gdy takie pytanie jest podniesione w sprawie zawisłej przed sądem krajowym, którego orzeczenia nie podlegają zaskarżeniu według prawa wewnętrznego, sąd ten jest zobowiązany wnieść sprawę do Trybunału.

Celem wyjaśnienia wszelkich wątpliwości należy wskazać, że na podstawie projektowanej regulacji sądowi administracyjnemu nie będzie przysługiwało uprawnienie do stwierdzenia

nieważności powołanych w przepisie decyzji Komisji Europejskiej. Tego rodzaju regulacja naruszałaby niezależność sądu administracyjnego, narzucając obligatoryjne działanie procesowe. Dodatkowo zgodnie z utrwalonym orzecznictwem TSUE, sąd krajowy państwa członkowskiego nie ma kompetencji orzekania o ważności aktów prawa UE.

Projektodawca zdecydował się również ograniczyć zastosowanie wskazanych powyżej regulacjiwyłącznie do decyzji Komisji Europejskiej, które dotyczą przekazywania danych osobowych do państw trzecich oraz organizacji międzynarodowych, nie chcąc dokonywać rozszerzającej wykładni wyroku TSUE. Jak zostało to już bowiem wskazane, wprowadzenie do projektu przedmiotowej regulacji uzasadnione jest treścią wyroku TSUE w sprawie Maxa Schremsa, stwierdzającego nieważność decyzji Komisji Europejskiej zatwierdzającej porozumienie Safe Habor wyrok (C-362/14), a więc obejmującego swoim zakresem przedmiotowym co do zasady sprawy dotyczące międzynarodowych transferów danych.

Rozdziału 8. Europejska współpraca administracyjna. Przepisy 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.

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.

Dokonywanie efektywnej współpracy wymaga dokładnego doprecyzowania zakresu zadań podejmowanych przez każdy z organów nadzorczych państw członkowskich. Projektowane przepisy projektu ustawy nakładają 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.

Rozdział 9. Postępowanie kontrolne. W przepisach rozdziału 9 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. W ocenie projektodawcy, celem wyeliminowania ryzyka jakichkolwiek nieprawidłowości w zakresie przeprowadzanych kontroli wzór legitymacji służbowej okazywanej w trakcie przeprowadzanej kontroli powinien zostać określony w drodze rozporządzenia. 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. Zakres udzielanych upoważnień do przeprowadzenia kontroli określają przepisyprojektu. Dla zapewnienia możliwości przeprowadzenia kontroli pod nieobecność kontrolowanego przewidziano, że upoważnienie do przeprowadzenia kontroli będzie mogło być okazane pracownikowi kontrolowanego lub przywołanemu świadkowi, którym powinien być funkcjonariusz publiczny. W związku ze stałym rozwojem nowych technologii oraz założeniami na jakich opiera się Rozporządzenie ochrona danych osobowych wymaga wiedzy z pogranicza prawa, sektora IT oraz analityki. Projektodawca dostrzega więc potrzebę skorzystania Prezesa Urzędu z zaplecza eksperckiego, przewidując możliwość upoważnienia przez niego do udziału w kontroli osobę posiadającą taką wiedzę. Zakres uprawnień kontrolujących oraz obowiązków kontrolowanych określa projekt. Projektodawca zdecydował się wprowadzić ograniczenie czasu przeprowadzania kontroli do godzin 6.00 – 22.00, uznając, iż ochrona danych osobowych nie będzie wymagała podjęcia aż tak nagłych czynności kontrolnych. Postanowiono zatem wyłączać z mocy ustawy możliwość przeprowadzenia kontroli poza ww. godzinami. Ważną i nową regulacją, mająca na celu skuteczne przeprowadzenie czynności kontrolnych, są przepisy pzowalającekontrolującym korzystać z pomocy funkcjonariuszy innych organów kontroli lub Policji. W szczególności należy wskazać, że policja zobowiązana będzie do udzielenia pomocy nie tylko w przypadkach o których mowa w art. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. 2017 poz. 2067), ale również gdy jest to konieczne gdy kontrolujący natrafi na opór, który utrudnia lub uniemożliwia mu wykonywanie kontroli, albo jeżeli istnieje uzasadnione przypuszczenie, że na taki opór natrafi. Uwzględniając dotychczasową praktykę działania GIODO sytuacje takie

występują rzadko, ale ich wystąpienie uniemożliwia skuteczne przeprowadzenie kontroli. Zgodnie z przepisami projektu kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Rozdział 10. Odpowiedzialność cywilna. Rozdział 10 projektu ustawy odnosi się do odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych. 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 37 odpowiedzialności odszkodowawczej w ogólnym rozporzą-

dzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich, Europejski Przegląd Sądowy z 2017, nr 5). W związku z powyższym projektowane regulacje dotyczą 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. 89 ust. 2 projektu wyraźnie przesądza, iż dochodzenie roszczeń w oparciu o art. 89 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. 89 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 projek-

todawca zdecydował się na wprowadzenie regulacji odrębnej w art. 89 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. Założeniem projektodawcy przy włączeniu do projektu art. 89 było ustanowienie alternatywnej i niekonkurencyjnej wobec roszczenia z art. 23 i 24 k.c. podstawy prawnej dochodzenia roszczeń z tytuły naruszenia ochrony danych osobowych. W tym zakresie wybór podstawy prawnej dochodzenia roszczeń należy więc do osoby której dane osobowe zostały naruszone z tym zastrzeżeniem, że taki wybór nie zawsze będzie możliwy. Nie każde naruszenie prawa do prywatności o którym mowa w art. 23 i 24 k.c. skutkuje bowiem naruszeniem ochrony danych osobowych i nie każde naruszenie danych osobowych skutkuje naruszeniem prywatności. Tytułem przykładu naruszeniem prywatności rozumianej powszechnie jako prawo do intymności, będzie podglądanie kogoś lornetką w jego prywatnym mieszkaniu, bez podstawy prawnej. O ile jednak działania kończą się wyłącznie na podglądaniu, bez utrwalania wizerunku osoby podglądanej, nie skutkują one naruszeniem zasad ochrony danych osobowych. Projekt nie mógłby być więc w takiej sytuacji podstawą dochodzenia jakichkolwiek roszczeń. Z drugiej strony jednym z przewidzianych przepisami Rozporządzenia nowych, nieznanych dzisiaj uprawnień jest prawo do przeniesienia danych osobowych. Zgodnie z art. 20 Rozporządzenia osoba, której dane dotyczą, ma prawo przesłać swoje dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Odmowa ze strony administratora zrealizowania żądania osoby której dane dotyczą przekazania ich wskazanemu przez taka osobę podmiotowi narusza zasady ochrony danych osobowych, ale nie narusza dobra osobistego jakim jest prywatność. Odmowa realizacji prawa do przeniesienia danych nie ingeruje bowiem w żadnym zakresie w sferę intymności człowieka. W takim przypadku podstawą prawną dochodzenia roszczeń będzie mógł więc być art. 89 projektu, ale już nie art. 23 i 24 k.c. Bez wątpienia są jednak naruszenia związane ochroną danych osobowych które mogą wiązać się jednocześnie z naruszeniami prywatności – wycieki danych osobowych. Należy zwrócić uwagę, iż art. 89 ust. 1 projektu dotyczy wyłącznie dokonanego naruszenia praw przysługujących na mocy przepisów o ochronie danych osobowych. W tej sytuacji przysługi-

wać będzie roszczenie o: - zaniechanie tego działania; - to aby ten kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. Projektowane przepisy mają charakter porządkowy i przesądza cywilnoprawny tryb dochodzenia roszczeń wskazanych w projekcie. 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. Decyzja o przyznaniu sądom okręgowym właściwości w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych podyktowana została względami ekonomiki w tym chęcią zapewnienia szybkości postępowania. Liczba spraw rozpatrywanych przez sądy okręgowe jest mniejsza niż sądy rejonowe. Przepis ten stanowi regulację szczególną względem art. 17 pkt 4 kodeksu postępowania cywilnego. Celem wprowadzenia przedmiotowych regulacji do projektu jest udrożnienie i przyspieszenie komunikacji pomiędzy sądami powszechnymi a Prezesem Urzędu. Należy zwrócić uwagę, iż wniesienie pozwu w sprawach, o których mowa w projekcie obliguje sąd – przed którym toczy się postępowanie - do zawiadomienia Prezesa Urzędu. Niemniej sąd może ale nie musi zawiesić toczącego się przed nim postępowania. W ocenie projektodawcy ważnym do wskazania jest również, że wprowadzenie do projektu wskazanych regulacji nie ma wpływu na toczące się obecnie postępowania.

Rozdział 11. Administracyjne kary pieniężne. Przepisy rozdziału 11 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.

Polski prawodawca skorzystał z możliwości jaką daje art. 83 ust. 7 Rozporządzenia i 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, Narodowy Bank Polski oraz Radę Polityki Pieniężnej i wysokość kar nie może przekroczyć 100 000 zł. Zarówno Narodowy Bank

Polski jak i Rada Polityki Pieniężnej są organami przewidzianymi w Konstytucji Rzeczpospolitej Polskiej i bez wątpienia są organami publicznymi. Jednocześnie jednak nie znajdują się one w katalogu podmiotów o których mowa w art. 9 ustawy o finansach publicznych, co wymusiło na projektodawcy ich enumeratywne wskazanie w projektowanym przepisie.

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, ograniczając maksymalny wymiar kary wymierzanej wobec instytucji kultury do 10 000 zł. 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. Muzea, teatry i podobne instytucje zwykle przetwarzają podstawowe dane osobowe, takie jak: imię, nazwisko, adres i dane kon-

taktowe. Dane te są potrzebne najczęściej w związku z korzy-staniem 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 pod-mioty 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.

Zgodnie z projektem ustawy Prezes Urzędu Ochrony Danych Osobowych „może na wniosek podmiotu ukaranego odroczyć uiszczenie kary pieniężnej albo rozłożyć ją na raty ze względu na ważny interes wnioskodawcy". Na podstawie projektu ustala się odsetki w wysokości 50% stawki odsetek za zwłokę. Wprowadzona na podstawie ww. przepisu ulga może spełniać przesłanki pomocy publicznej określone w art. 107 ust. 1 TFUE, gdyż: może powodować uszczuplenie dochodów państwa, ma charakter selektywny (skierowana jest do określonych podmiotów), może stanowić dla zgłaszających korzyść, której nie uzyskaliby w normalnych warunkach rynkowych, a także - jako że wśród beneficjentów tej ulgi znajdują się przedsiębiorcy działający na rynkach otwartych na konkurencję - może zakłócić lub grozić zakłóceniem konkurencji i wpłynąć na wymianę handlową między państwami członkowskimi UE.

Rozdział 12. Przepisy karne. Rozdział 12 projektu wprowadza przepisy karne. Generalnym 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 na podstawie przepisów Kodeksu Karnego. Zgodnie z treścią projektowanych przepisów, kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, będzie podlegał grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Przepisy penalizują również przetwarzanie zwykłych i szczególnych kategorii danych (z art. 9 Rozporządzenia) bez podstawy prawnej. Mając na względzie dobro podmiotów danych oraz wagę naruszenia, jakim jest przetwarzanie danych osobowych, uznano, że przetwarzanie danych bez podstawy prawnej, a więc nieuprawnione i umyślne przetwarzanie, powinno być zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności. Projektodawca zdecydował się jedynie rozróżnić maksymalny wymiar możliwej kary od kategorii przetwarzanych danych, w ślad za intencją ustawodawcy unijnego który wprowadza dwie kategorie danych: danych szczególnie chronionych oraz danych zwykłych. Jednocześnie projektodawca nie zdecydował się zmienić obowiązujących obecnie maksymalnych wymiarów kar wskazując je na poziomie dwóch lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych zwykłych oraz trzech lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych wrażliwych. 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".

Rozdział 13. Przepisy zmieniające. Przepisy uzasadnianego rozdziału co do zasady pełnią rolę techniczno-legislacyjną i mają na celu zmianę nazwy organu z Generalnego Inspektora

Ochrony Danych Osobowych na Prezesa Urzędu Ochrony Danych Osobowych, administratora bezpieczeństwa informacji na inspektora ochrony danych oraz odwołują odwołania do obowiązującej ustawy.

Należy wskazać, iż spory w których występują organy administracji publicznej nieposiadające organów wyższego stopnia jak to ma miejsce w przypadku Prezesa Urzędu Ochrony Danych Osobowych oraz nie należą do innych organów zdefiniowanych w art. 22 Kodeksu rozstrzyga sąd administracyjny. Z uwagi na fakt, iż chodzi o ograny które zazwyczaj na mocy przepisów ustrojowych cechują się niezależnością i swoistymi regulacjami posłużono się pojęciem „sporu kompetencyjnego" zamiast sporu o właściwość. Jak wskazuje się w doktrynie rozróżnienie pojęć „spór o właściwość" oraz „spór kompetencyjny" ma pełne umocowanie w konstrukcjach prawa ustrojowego. O ile przy sporze o właściwość chodzi wyłącznie o podział właściwości pomiędzy organami należącymi do tego samego systemu ustrojowego, to przy sporach kompetencyjnych przedmiotem jest rozdzielenie kompetencji pomiędzy różne systemy ustrojowe administracji publicznej (B. Adamiak, J. Borkowski Komentarz do kodeksu postępowania administracyjnego, wyd. C. H. Beck 2017 r. wydanie 15).

W konsekwencji w ustawie – Prawo o postępowaniu przed sądami administracyjnymi należy dodać odpowiednią regulację umożliwiającą sądom administracyjnym rozstrzyganie ww. sporów kompetencyjnych. W tym celu ustawodawca postanowił, podobnie jak w przypadku organów jednostek samorządu terytorialnego, wprowadzić zasadę, iż spory kompetencyjne miedzy organami państwowymi prowadzącymi postępowania administracyjne niebędącymi organami administracji rządowej, organami jednostek samorządu terytorialnego i samorządowymi kolegiami odwoławczymi oraz pomiędzy tymi organami a organami administracji rządowej, o ile odrębna ustawa nie stanowi inaczej będzie rozstrzygał Sąd administracyjny. W przypadku ustawy o Prawo o postępowaniu przed sądami administracyjnymi posłużono się innym pojęciem niż w przepisach kodeksu postepowania administracyjnego. Ponieważ PPSA nie reguluje swoim zakresem sporów kompetencyjnych pomiędzy organami administracji rządowej, ta kwestia jest regulowana na gruncie kodeksu postepowania administracyjnego. Zasadne jest zatem odwołanie się do sporów kompetencyjnych jedynie w stosunku do organów nie będących organami administracji rządowej, a będącymi organami państwowymi innymi niż organy jednostek samorządu teatralnego, samorządowymi kolegami odwoławczymi oraz pomiędzy tymi organami a organami administracji rządowej. Z uwagi na pozy-

cję ustrojową ww. organów właściwym sądem administracyjnym jest Naczelny Sąd Administracyjny.

Projektodawca w przepisach zmieniających zdecydował się utrzymać szczególną pozycję Prezesa Urzędu Ochrony Danych Osobowych jako organu o zagwarantowanej autonomii budżetowej stosowanie do art. 139 ust. 2 ustawy o finansach publicznych. Mimo, że Prezes Urzędu nie jest organem konstytucyjnym, wymóg zapewnienia organowi autonomii budżetowej wynika wprost z rozporządzenia 2016/679. Zgodnie z art. 52 ust. 6 rozporządzenia 2016/679 „każde państwo członkowskie zapewnia, by każdy organ nadzorczy podlegał kontroli finansowej w sposób nienaruszający jego niezależności oraz dysponował odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego". W ocenie projektodawcy, w polskim systemie prawnym powyższy wymóg może być zagwarantowany właśnie autonomią budżetową, a więc poprzez utrzymanie w tym zakresie pozycji posiadanej obecnie przez GIODO.

Rozdział 14. Przepisy przejściowe i dostosowujące.

Projektodawca zapewniając sprawność działania systemu ochrony danych osobowych oraz dostrzegając ogromny wpływ na jego działania inspektorów ochrony danych zdecydował się wprowadzić przepisy przejściowe w tym zakresie. Dostrzegając trudność w możliwości zgłoszenia wszystkich osób pełniących dotychczas funkcję administratorów bezpieczeństwa informacji jako inspektorów ochrony danych, osoby pełniące funkcję administratorów bezpieczeństwa informacji, będą mieli na to czas do 1 września 2018 r. Trudność w dokonaniu takiego zgłoszenia w dniu 25 maja może powstać zarówno po stronie administratorów, jak i Prezesa Urzędu, który otrzymałby ogromną ilość nowych zgłoszeń w stosunkowo krótkim czasie. W ocenie projektodawcy nie jest jednak możliwe przesądzenie, że wszystkie osoby pełniące funkcję administratorów bezpieczeństwa informacji, stają się z data wejścia w życie projektowanej ustawy inspektorami ochrony danych, z uwagi do dużą liczbę nowych obowiązków wynikających z rozporządzenia 2016/679. Wymaga ona podjęcia świadomej decyzji po stronie osoby chcącej pełnić funkcję inspektora ochrony danych.

Projektodawca przewidując w projekcie ustanowienie organu – Prezesa Urzędu Ochrony Danych Osobowych widzi również konieczność zapewnienia pełnej ciągłości działania organu. W związku z powyższym, projektowane przepisy przewidują, że z dniem wejścia w życie

ustawy pracownicy zatrudnieni w Biurze Generalnego Inspektora Ochrony Danych Osobowych stają się pracownikami Urzędu Ochrony Danych Osobowych, mienie Skarbu Państwa będące we władaniu Generalnego Inspektora Ochrony Danych Osobowych staje się mieniem Prezesa Urzędu Ochrony Danych Osobowych, a należności i zobowiązania Generalnego Inspektora Ochrony Danych Osobowych z dniem wejścia w życie ustawy stają się należnościami i zobowiązaniami Prezesa Urzędu Ochrony Danych Osobowych. Przepisy projektu wskazują bardzo wyraźnie, że Generalny Inspektor Ochrony Danych Osobowych staje się Prezesem Urzędu Ochrony Danych Osobowych i pełni swoją funkcję do czasu upływu kadencji na którą został powołany. Tym samym w projekcie nie przewiduje się jakiegokolwiek skrócenia kadencji osoby obecnie pełniącej funkcję GIODO. W Polsce osoba pełniąca funkcję GIODO została powołana na to stanowisko przez Sejm RP 9 kwietnia 2015 r., a Senat zaakceptował ten wybór 16 kwietnia 2015 r. Natomiast od dnia złożenia ślubowania przed Sejmem, tj. od 22 kwietnia 2015 r., zgodnie z obowiązującą ustawą o ochronie danych osobowych, rozpoczęła się czteroletnia, kadencja GIODO. Kadencja organu upłynie więc w kwietniu 2019 r.

Na szczególną uwagę zasługuje również fakt, że w ocenie projektodawcy dane zgromadzone w rejestrze zbiorów danych osobowych oraz rejestrze administratorów bezpieczeństwa informacji po wejściu w życie projektowanej ustawy powinny podlegać archiwizacji. Przepisy rozporządzenia 2016/679 oraz projektowanej ustawy nie przewidują bowiem rejestracji zbiorów danych osobowych oraz inspektorów ochrony danych. Za archiwizacją danych zgromadzonych w rejestrach przemawia natomiast interes publiczny – rejestry zawierające setki tysięcy rekordów danych stanowią gromadzony przez lata obraz działania państwa w sektorze ochrony danych osobowych. Dodatkowo, brak rejestracji zbiorów danych osobowych do dnia wejścia w życie projektowanej ustawy stanowi przestępstwo, zagrożone karą grzywny, ograniczenia wolności bądź pozbawienia wolności do roku. Może okazać się więc koniecznym dokonanie oceny faktu zarejestrowania zbioru danych osobowych przez dany podmiot przed wejściem w życie projektowanej ustawy. Rejestry zawierają również informacje umożliwiające nawiązanie kontaktu organu nadzorczego z podmiotem dokonującym rejestracji. Należy również wskazać, że wprowadzenie do projektu rozwiązanie nie narusza przewidzianej w art. 5 ust. 1 lit. c rozporządzenia 2016/679 zasady „minimalizacji danych". Gromadzone obecnie w rejestrze dane osobowe mają bardzo ograniczony zakres. Rejestry zawierają jedynie dane osobowe kategorii: imię, nazwisko, adres oraz pełniona funkcja administratora

bezpieczeństwa informacji. W niektórych przypadkach danymi osobowymi mogą być również wskazane w rejestrach dane kontaktowe.

Rozdział 15. Przepisy końcowe.

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.

Przepisy projektowanego rozdziału przewidują zgodnie z zasadami poprawnej legislacji maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy w okresie 10 letnim od wejścia w życie projektowanej ustawy. Obliczenia zostały podjęte na podstawie dołączonej do projektu Oceny Skutków Regulacji. 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, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248). W trybie przepisów ww. ustawy nie wpłynęły wnioski.