Wprowadzenie
do projektu części przepisów ustawy o ochronie danych osobowych

Przepisy nowej ustawy o ochronie danych osobowych, mają zapewnić skuteczne stosowanie w polskim porządku prawnym 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), (dalej: rozporządzenie 2016/679). Udostępnieniu przez Ministra Cyfryzacji podlega projekt części przepisów regulujących: zagadnienia ogólne (niektóre przepisy), zagadnienia związane z postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych, europejską współpracą administracyjną, postępowaniem kontrolnym, administracyjnymi karami pieniężnymi, odpowiedzialnością cywilną i inspektorami ochrony danych.

Treść przepisów rozporządzenia 2016/679 skłoniła projektodawcę do zaproponowania w projekcie nowej nazwy powoływanego organu ochrony danych osobowych – Prezes Urzędu Ochrony Danych Osobowych. Po pierwsze, rozporządzenie 2016/679 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 2016/679. Jednocześnie brak jest jednak jakiegokolwiek związku ustrojowego pomiędzy takimi osobami a przyszłym organem nadzorczym odpowiadającym za egzekwowanie w Polsce przestrzegania przepisów rozporządzenia 2016/679. Przejęcie obecnej nazwy organu wprowadzałoby w tym zakresie w błąd, w tym co do ich pozycji ustrojowej. Zgodnie bowiem z art. 38 ust. 3 rozporządzenia 2016/679 inspektorzy ochrony danych muszą być niezależni. Po drugie utrzymanie obecnej nazwy - Generalny Inspektor Ochrony Danych Osobowych powodowałoby niejako konieczność nazwania pracowników biura, którzy w imieniu organu przeprowadzają postępowanie kontrolne inspektorami. 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 powoływanych wewnątrz struktury

organizacyjnej administratorów i podmiotów przetwarzających, co nie jest niedopuszczalne. Uwzględniając powyższe, odstąpiono również od nazywania pracowników organu nadzorczego przeprowadzających w jego imieniu czynności kontrolne inspektorami, na rzecz nazwania ich kontrolującymi. W ocenie projektodawcy uwzględniając powyższe, najwłaściwszym jest użycie nazwy wykorzystywanej w Polsce najczęściej i najłatwiejszej do przyswojenia dla obywateli – Prezes Urzędu Ochrony Danych Osobowych (dalej: Prezes Urzędu).

Udostępniony projekt części przepisów ustawy, otwiera rozdział „Przepisy ogólne". W rozdziale tym są aktualnie zamieszczone dwa przepisy. Są to przepisy dotyczące wieku dziecka, gdy konieczne jest odebranie zgody rodzica na przetwarzanie jego danych w przypadku usług społeczeństwa informacyjnego, oraz dotyczące technicznych i organizacyjnych środków zabezpieczenia danych osobowych. Odnosząc się do pierwszego z zagadnień, art. 8 rozporządzenia 2016/679 uprawnia każde z państw członkowskich do przewidzenia niższej niż 16 lat granicy wieku dziecka, gdy przetwarzanie jego danych osobowych, w przypadku usług społeczeństwa informacyjnego, wymaga zgody rodziców bądź opiekunów prawnych. Zgodnie z art. 15 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. z 2016 r. poz. 380, z późn. zm.) osoba, która ukończyła 13 lat ma ograniczoną zdolność do czynności prawnych, a zatem może zawierać umowy w drobnych bieżących sprawach życia codziennego, może także rozporządzać swoim zarobkiem. W ocenie projektodawcy w tym kontekście uzasadnione jest przyjęcie granicy lat 13 także dla skutecznego wyrażenia przez dziecko zgody na przetwarzanie dotyczących go danych osobowych, w związku z kierowanymi bezpośrednio do dziecka usługami społeczeństwa informacyjnego. Nie ma powodu, aby przyjąć, że osoba mogąca rozporządzić swoim zarobkiem oraz zawierać drobne umowy, nie była jednocześnie uprawniona do wyrażenia zgody na przetwarzanie dotyczących jej danych osobowych, szczególnie, że zgodnie z przepisami rozporządzenia 2016/679 zgodę można w każdym czasie wycofać. Odnosząc się do drugiego z uregulowanych zagadnień, w ocenie projektodawcy koniecznym jest zobowiązanie Prezesa Urzędu do wydawania niewiążących dobrych praktyk w zakresie możliwych do zastosowania zabezpieczeń przetwarzania danych. Należy jednak podkreślić niewiążący charakter rekomendacji zawartych w dobrych praktykach. Ich zastosowanie nie może ograniczać przewidzianej w rozporządzeniu 2016/679 ochrony danych osobowych opartej na każdorazowej ocenie ryzyka związanego z ich przetwarzaniem. Administrator bądź podmiot przetwarzający nie będzie więc zwolniony od dokonania oceny, jakie środki zabezpieczające dane osobowe powinny być w danym stanie faktycznym zastosowane – czasami koniecznym może okazać się wdrożenie środków dalej idących niż przewidziane w dobrych praktykach. Ich wydawane wpłynie jednak na większe poczucie pewności prawnej, zwiększając stopień przestrzegania przez administratorów i podmioty przetwarzające przepisów

rozporządzenia 2016/679. Przewidziany w projektowanej ustawie obowiązek formułowania takich niewiążących rekomendacji jest oparty o art. 57 ust. 1 lit. d rozporządzenia 2016/679, zgodnie z którym organ nadzorczy na swoim terytorium upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy rozporządzenia. Należy jednak jeszcze raz podkreślić, że dobre praktyki nie powinny mieć charakteru regulacyjnego, a jedynie informacyjny. Celem zawartych w dobrych praktykach rekomendacji jest wsparcie administratorów i podmiotów przetwarzających w ocenie, jakie środki techniczne i organizacyjne mogą być wdrożone w celu adekwatnego zaadresowania zidentyfikowanego ryzyka przetwarzania danych osobowych. Z faktu działania w zgodzie z rekomendacjami nie powinny też wynikać żadne gwarancje dla administratorów ani podmiotów przetwarzających. Jakiekolwiek formalne związanie organu wydanymi rekomendacjami powodowałoby konieczność uznania, że rekomendacje mają w istocie charakter regulacyjny, co mogłoby zostać uznane za niezgodne z prawem UE.

Uwzględniając szczególny cel projektowanej ustawy, jakim jest zapewnienie w Polsce skutecznym egzekwowania ochrony danych osobowych będącej jednym z praw podstawowych, zdecydowano się przyznać stronom postępowania prowadzonego przed Prezesem Urzędu szerokiego katalogu uprawnień procesowych. W projekcie zaproponowano by postępowanie w sprawach ochrony danych osobowych było prowadzone na podstawie przepisów ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2016 r. poz. 23, późn. zm.)(dalej: KPA), zawierającej szeroki katalog instytucji prawnych gwarantujących poszanowanie takich uprawnień. Projektowane przepisy przewidują jednak pewne odrębności względem zasad przewidzianych w KPA, które podzielić można na dwie grupy.

Do pierwszej z nich należą przepisy, wprowadzające regulacje szczególne co uzasadnione jest dostosowaniem prowadzonego postępowania do specyfiki naruszenia, jakim jest naruszenie przepisów o ochronie danych osobowych. W tym też celu przewidziano uprawnienie organizacji społecznej do wystąpienia z żądaniem wszczęcia postępowania bądź udziału w postępowaniu, nie tylko w przypadku gdy przemawia za tym interes społeczny, o czym stanowi art. 31 § 1 KPA, ale również gdy przemawia za tym interes osoby, której prawa zostały naruszone. Projekt przepisów przewiduje również możliwość wyznaczenia stronie terminu do przedstawienia dowodu będącego w jej posiadaniu. Uwzględniając szczególny wymiar sądowej kontroli działań podejmowanych przez Prezesa Urzędu, zmierzających często do wymierzania administracyjnych kar pieniężnych, sąd dysponować musi szerokim materiałem dowodowym zgromadzonym w toku postępowania administracyjnego. Do projektu wprowadzone zostało więc postanowienie, w świetle którego Prezes Urzędu może wyznaczyć stronie termin do przedstawienia każdego dowodu będącego w

jej posiadaniu. Szczególnej ochronie powinny podlegać jednak informacje objęte tajemnicą prawnie chronioną w tym również tajemnicą przedsiębiorstwa. Uwzględniając często bardzo dużą wartość rynkową informacji objętych takimi tajemnicami bądź ryzyko związane z ich ujawnieniem, należy wyeliminować przypadki gdy strona wolała będzie ponieść odpowiedzialność z tytułu odmowy udostępnienia danych treści, niż przekazać je Prezesowi Urzędu. Podstawą do przewidzenia szczególnych regulacji w tym zakresie jest art. 90 rozporządzenia 2016/679. W wielu stanach faktycznych nawet najszybciej prowadzone postępowanie administracyjne w sprawach naruszenia przepisów o ochronie danych może okazać się zbyt długim, by usunąć naruszenie ochrony danych osobowych. W związku z powyższym zdecydowano się na wprowadzenie do projektowanej ustawy przepisu uprawniającego Prezesa Urzędu do wydania postanowienia zobowiązującego podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych wskazując dopuszczalny zakres tego przetwarzania. Podobne rozwiązanie prawne zastosowane zostało przez ustawodawcę przykładowo w ustawie z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. 2017 poz. 229). Postanowienie byłoby środkiem tymczasowym wydawanym przez Prezesa Urzędu, o którym mowa w art. 61 ust. 8, 62 ust. 7, 66 ust. 1 rozporządzenia 2016/679. Postanowienie to obowiązywać ma przez czas oznaczony w postanowieniu, jednak nie dłużej niż do czasu wydania decyzji kończącej postępowanie w sprawie. Projektodawca świadomie odstąpił od wprowadzenia możliwości odrębnego zaskarżenia postanowienia. Najwłaściwszym wydaje się bowiem wprowadzenie rozwiązania, w świetle którego kontrola zasadności wydania postanowienia podejmowana byłaby przez sąd w związku z rozpatrywaniem przez niego skargi na decyzję Prezesa Urzędu. Uznanie przez sąd w wyroku niezasadności wydania postanowienia, będzie mogło być podstawą do skierowania wobec Prezesa Urzędu roszczeń cywilnoprawnych . Projektowane przepisy niezależnie od środków prawnych (decyzji) których wydawanie przysługuje Prezesowi Urzędu na mocy art. 26 projektu, uprawniają organ do udzielenia w drodze decyzji administracyjnej upomnienia. Organ uprawniony będzie do jego udzielenia w przypadku, gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia. Przepis ma zapewnić skutecznym stosowanie art. 58 ust. 2 lit. b rozporządzenia 2016/679 w świetle którego każdemu organowi nadzorczemu przysługuje uprawnienie do udzielania upomnień w przypadku naruszenia przepisów rozporządzenia przez operacje przetwarzania. W przeciwieństwie do wskazanych w art. 58 ust. 2 lit. a rozporządzenia 2016/679 ostrzeżeń, upomnienie organ może wydać wyłącznie w przypadku *naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania.* Prezes Urzędu w toku prowadzonego postępowania administracyjnego musi więc w pierwszej kolejności przesądzić, że do naruszenia

takiego doszło. Powyższe determinuje konieczność umieszczenia uprawnienia do udzielania przez Prezesa Urzędu przedmiotowego upomnienia w przepisach regulujących postępowanie administracyjne prowadzone przed Prezesem Urzędu i nadanie mu formy zaskarżalnej decyzji administracyjnej. Celem przyśpieszenia postępowania prowadzonego przed Prezesem Urzędu, projektodawca zdecydował się w art. 29 projektowanej ustawy nadać z mocy prawa wydawanym przez Prezesa Urzędu decyzjom rygor natychmiastowej wykonalności. Powyższe, ma odciążyć Prezesa Urzędu od konieczności poodejmowania czynności administracyjnych zmierzających do każdorazowego nadawania decyzjom rygoru natychmiastowej wykonalności. Rozwiązanie takie jest w pełni uzasadnione charakterem chronionego przez wydawane decyzje dobra, którym jest prawo podstawowe do ochrony danych osobowych wymagające szczególnego zabezpieczenia. Uwzględniając jednak przewidziane w rozporządzeniu 2016/679 uprawnienie do nakładania przez Prezesa Urzędu wysokich administracyjnych kar pieniężnych, odstąpiono od nadawania z mocy prawa rygoru natychmiastowej wykonalności decyzjom nakładającym takie kary. Mogłoby to skutkować niepowetowanymi stratami po stronie administratorów bądź podmiotów przetwarzających wobec których decyzje takie zostałyby wydane. W projekcie odstąpiono od utrzymania dwuinstancyjności postępowania w sprawach naruszenia przepisów o ochronie danych osobowych, na rzecz postępowania jednoinstancyjnego. Możliwość wprowadzenia w przepisach szczególnych jednoinstancyjności postępowania administracyjnego przewidziana została wprost w przepisach ustawy nowelizującej KPA, która znajduje się aktualnie na etapie prac parlamentarnych. Projektując takie rozwiązanie w pierwszej kolejności oparto się na statystykach związanych z obecnym czasem trwania postępowań w sprawach ochrony danych osobowych. W tym celu analizie poddane zostały wyroki wydawane przez Naczelny Sąd Administracyjny za 2015 r. (ostatni rok, w którym dane w chwili podejmowanej analizy były w pełni kompletne). Wyniki analizy wskazują, że średni czas oczekiwania na decyzję Generalnego Inspektora Ochrony Danych Osobowych w pierwszej instancji wyniósł 295,75 dni, a na decyzję w drugiej instancji 142,30 dni. Uwzględniając szczególny charakter postępowań dotyczących naruszenia zasad ochrony danych osobowych czas konieczny do uzyskania decyzji ostatecznej umożliwiającej skierowanie skargi do sądu jest w chwili obecnej zbyt długi. Zniesienie dwuinstancyjności ma więc zapewnić obywatelom możliwość szybszego uzyskania sądowej ochrony swoich praw. Prezesowi Urzędu przyznane zostało jednak w art. 31 projektu uprawnienie do autokontroli wydanej decyzji. Prezes Urzędu może w terminie 30 dni od dnia wniesienia skargi uchylić zaskarżoną decyzję i wydać nową. Projektodawca zdecydował się na pozostawienie dzisiejszego sądowo-administracyjnego modelu kontroli rozstrzygnięć wydawanych przez Prezesa Urzędu. Podejmując taką decyzję rozważono wszystkie możliwości, w tym również poddania spraw z zakresu ochrony

danych osobowych sądownictwu powszechnemu bądź sądowi wyspecjalizowanemu jakim jest Sąd Ochrony Konkurencji i Konsumentów. Przyznanie właściwości do orzekania w sprawach naruszenia przepisów o ochronie danych osobowych sądom administracyjnym, jest w ocenie projektodawcy najwłaściwszym. Za podjęciem takiej decyzji przemówiło w pierwszej kolejności ogromne doświadczenie polskich sądów administracyjnych w orzekaniu od dwudziestu lat w sprawach ochrony danych osobowych. Po drugie przekonanie, że sądownictwo administracyjne przy obecnym ogromnym obciążeniu sądów powszechnych, jest w stanie zapewnić szybszą kontrolę rozstrzygnięć Prezesa Urzędu. Po trzecie wreszcie, rozporządzenie 2016/679 w art. 79 wymaga od państw członkowskich wprowadzenia odrębnej drogi dochodzenia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych – poprzez przyznanie uprawnienia do skierowania „skargi" bezpośrednio do sądu z pominięciem organu nadzorczego (Prezesa Urzędu). Jednocześnie skorzystanie z takiego uprawnienia nie powinno w ocenie projektodawcy wyłączać możliwości wystąpienia ze skargą do Prezesa Urzędu, a sąd powinien mieć prawo do wydania wyroku niezależnie od rozstrzygnięcia wydanego przez Prezesa Urzędu. W świetle powyższego, koniecznym jest poddanie obu możliwych dróg dochodzenia ochrony swoich danych osobowych odpowiednio różnym pionom sądownictwa. W związku z powyższym, o ile skarga od decyzji Prezesa Urzędu powinna przysługiwać do sądu administracyjnego, o tyle właściwym do orzekania w przedmiocie skarg złożonych na podstawie art. 79 rozporządzenia 2016/679 powinny być sądy powszechne. Uwzględniając jednak zakres przyznanych sądom administracyjnym uprawnień do kontroli legalności zaskarżanych rozstrzygnięć, oraz treść wynikających z prawa unijnego warunków wymierzania administracyjnej kary pieniężnej (art. 83 rozporządzenia 2016/679), ogromne znacznie Prezes Urzędu powinien przywiązywać do zebrania w toku postępowania dowodów. Dowodów przemawiających nie tylko za wymierzeniem administracyjnej kary pieniężnej, ale również wymierzeniem kary o takiej a nie innej wysokości. Właśnie powyższe zdeterminowało decyzję prawodawcy o przyznaniu w projektowanych przepisach Prezesowi Urzędu wskazanego już uprawnienia do wyznaczenia stronie terminu do przedstawienia dowodu będącego w jej posiadaniu. Ogromne znaczenie Prezes Urzędu przywiązywać powinien również do wyczerpującego uzasadnienia wydawanych przez siebie rozstrzygnięć.

Do drugiej grupy odrębności względem KPA wprowadzonych przez projektodawcę należą przypadki tych przepisów, których stosowanie w postępowaniu w sprawach naruszenia przepisów o ochronie danych osobowych zostało wprost wyłączone. Należy do nich w pierwszej kolejności art. 13 oraz art. 114 – 122 KPA dotyczące ugody administracyjnej. Istota naruszenia, jakim jest naruszenie przepisów o ochronie danych osobowych wyłącza możliwość ugodzenia się pomiędzy osobą której prawa zostały naruszone a naruszycielem. Projektodawca przewiduje również

zwolnienie Prezesa Urzędu z obowiązku prowadzenia metryk (art. 66 a). Wyłączenie stanowi wzmocnienie postulatu ustawodawcy unijnego wyrażonego chociażby w motywie 89 rozporządzenia 2016/679 o konieczności rezygnacji ze znacznych obciążeń administracyjnych organu, nie zawsze przyczyniających się do poprawy ochrony danych osobowych.

Rozporządzenie 2016/679 wprowadza złożone mechanizmy europejskiej współpracy administracyjnej w sprawach z zakresu ochrony danych osobowych. Projektodawca doszedł w tym zakresie do wniosku, że istotą wprowadzenia do rozporządzenia 2016/679 rozdziału VII „współpraca i spójność" było zunifikowanie mechanizmów współpracy, czyniąc ją łatwiejszą. Wprowadzenie jakichkolwiek odrębności na poziomie krajowym w tym zakresie mogłoby znacznie utrudnić a nawet uniemożliwić jej prowadzenie. Propozycje przepisów dotyczą więc wyłącznie tych zagadnień, bez których w ocenie projektodawcy prowadzenie takiej współpracy nie byłoby możliwe. Do pierwszych z nich należy rygor językowy prowadzonej współpracy. Każda formalna korespondencja (tj. prowadzona w ramach mechanizmów współpracy, o których mowa w rozdziale VII rozporządzenia 2016/679) powinna być prowadzona w języku urzędowym danego państwa członkowskiego bądź w języku angielskim. Uwzględniając jednak ochronę interesów stron prowadzonego postępowania, każdy z takich dokumentów powinien być również przetłumaczony na język polski i wraz z dokumentem w języku obcym znajdować się w aktach sprawy. Projektodawca odstąpił od uregulowania zasad językowych prowadzenia współpracy z organami i instytucjami Unii Europejskiej, wynika ona bowiem z właściwych przepisów prawa unijnego. W projekcie Projektodawca odstąpiono również od uregulowania zasad językowych prowadzenia współpracy organów nadzorczych innych państw członkowskich z Prezesem Urzędu, gdyż inne państwa członkowskie nie mogą być adresatami jakichkolwiek praw bądź obowiązków wynikających z polskiego porządku prawnego. Uwzględniając, że ustawodawca unijny w art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 rozporządzenia 2016/679 nie przesądził wprost w jakiej prawnej formie działają organy nadzorcze państw członkowskich wydając środki tymczasowe, projektodawca przewidział, że w polskim porządku prawnym będzie to postanowienie. Minister Cyfryzacji zapewniając w pełni skutecznym stosowanie przez Prezesa Urzędu art. 62 ust. 1 rozporządzenia 2016/679 przewidział również w projekcie wprost, że Prezes Urzędu dokonuje z organem nadzorczym innego państwa członkowskiego Unii Europejskiej ustaleń dotyczących wspólnej operacji i niezwłocznie sporządza wykaz ustaleń.

Minister Cyfryzacji przewidział w projektowanej ustawie rozbudowane przepisy regulujące zasady prowadzenia przez Prezesa Urzędu postępowania kontrolnego, dostrzegając istotną rolę przeprowadzanych kontroli dla skutecznego egzekwowania w Polsce ochrony danych osobowych. Jednocześnie rozporządzenie 2016/679 czyniąc zadość zasadzie autonomii proceduralnej oraz

instytucjonalnej państw członkowskich, przyznało państwom członkowskim pełną swobodę w określeniu zasad prowadzenia takiej kontroli. W art. 58 ust. 1 lit. b wskazano jedynie, że każdemu organowi nadzorczemu (Prezesowi Urzędu) przysługuje uprawnienie do prowadzenia postępowań w formie audytów. Mimo, że w polskim porządku prawnym termin „audyt" oraz „kontrola" nie są ze sobą tożsame, projektodawca uznał, że ratio legis powołanego przepisu unijnego tworzonego przecież w oderwaniu od tradycji prawnych pojedynczych państw członkowskich i będącym określeniem uniwersalnym dla wszystkich państw, przemawia za uznaniem, że na gruncie polskiego porządku prawnego adekwatnym terminem będzie termin „kontrola". Art. 36 projektowanej ustawy wskazuje, że kontrola może być prowadzona w trzech sytuacjach. Pierwszą z nich jest kontrola planowa, zgodnie ze stworzonym uprzednio przez Prezesa Urzędu planem kontroli i bez wszczynania jakiegokolwiek postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. W ocenie projektodawcy prowadzenie takich kontroli pozwala na skuteczne reagowanie na informacje o powtarzających się w określonych sektorach naruszeniach przepisów o ochronie danych osobowych. Drugą z możliwych kontroli jest kontrola doraźna, przeprowadzana poza planem kontroli, również bez wszczynania jednak jakiegokolwiek postępowania. Źródłem takiej kontroli mogą być chociażby doniesienia prasowe. Do trzeciej z rodzajów kontroli należą kontrole przeprowadzane jako jeden ze środków przysługujących Prezesowi Urzędu w toku prowadzonego postępowania administracyjnego. Zgodnie bowiem z art. 23 projektowanych przepisów, postępowanie kontrolne może być prowadzone w związku z toczącym się postępowaniem administracyjnym. Celem przyśpieszenia postępowań prowadzonych w związku z naruszeniami przepisów o ochronie danych osobowych projektodawca przewidział w art. 45, że postępowanie kontrolne nie może trwać dłużej niż miesiąc. Aby rozstrzygnąć wszelkie wątpliwości, projektowany przepis wskazuje wprost, że termin rozpoczyna swój bieg z chwilą podjęcia przez Prezesa Urzędu pierwszych czynności kontrolnych a kończy w dniu podpisania protokołu kontrolnego przez kontrolowanego albo w dniu dokonania wzmianki, o odmowie takiego podpisu. We wskazanym terminie Prezes Urzędu musi podjąć więc nie tylko wszystkie czynności kontrolne, ale zakończyć postępowanie kontrole. W sytuacji, gdy postępowanie kontrolne prowadzone było poza postępowaniem administracyjnym (tzw. kontrola planowa lub kontrola doraźna), w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych Prezes Urzędu powinien niezwłocznie wszcząć postępowanie administracyjne. W przypadku z kolei, gdy prowadzone postępowanie administracyjne wymaga przeprowadzenia takiego postępowania kontrolnego, czasu przeprowadzenia takiego postępowania nie powinno się wliczać do terminów, o których mowa w art. 35 KPA. W ocenie projektodawcy do powyższego terminu na podjęcie postępowania kontrolnego podejść powinno się jednak szczególnie

restrykcyjnie, a postępowanie kontrolne powinno trwać najkrócej jak to możliwe, nie dłużej jednak niż miesiąc. Projekt przepisów przewiduje również możliwość żądania przez Prezesa Urzędu w toku postępowania kontrolnego złożenia pisemnych lub ustnych wyjaśnień oraz wezwania i przesłuchania w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego (art. 40 ust. 1 pkt 4 projektu) oraz sporządzania kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informatycznych lub teleinformatycznych służących do przetwarzania danych (art. 40 ust. 2 projektu). Należy jednak pamiętać, że działania takie ograniczone są obowiązkiem zapewnienia ochrony tajemnicy przedsiębiorstwa oraz innych tajemnic prawnie chronionych. Projektodawca w związku z podejmowanymi konsultacjami pozyskał informację, o częstym utrudnianiu możliwości przeprowadzenia dzisiaj przez Generalnego Inspektora postępowania kontrolnego. W świetle powyższego, projektodawca przewidział w projektowanych przepisach wprost, że w toku kontroli kontrolujący może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji a organy kontroli państwowej lub Policja wykonują czynności na polecenie kontrolującego. W projekcie ustawy przesądzono wprost zakres zastosowania do postępowania kontrolnego prowadzonego na podstawie projektowanych przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2016 r. poz. 1829, 1948, 1997 i 2255). Projektowane przepisy wskazują więc wprost, że ustawa ta znajduje zastosowanie z wyłączeniem jej art. 79, art. 82 i art. 83. W efekcie, Prezes Urzędu będzie uprawniony do przeprowadzania kontroli bez uprzedniego zawiadomienia o tym fakcie kontrolowanego. Prowadzenie postępowania kontrolnego po uprzednim zawiadomieniu w wielu przypadkach może czynić bowiem niewiarygodnym informacje uzyskane w toku takich czynności. Postępowanie kontrolne w sprawach związanych z potencjalnym naruszeniem prawa podstawowego jakim jest ochrona danych osobowych nie powinno być również utrudnione faktem prowadzenia w tym samym czasie jakiejkolwiek innej kontroli ani przekroczeniem czasu trwania kontroli wobec danego przedsiębiorcy w roku kalendarzowym – właściwe przepisy zostały więc w tym zakresie wyłączone.

W ocenie projektodawcy wszystkie przewidziane w art. 83 rozporządzenia 2016/679 ogólne warunki nakładania administracyjnych kar pieniężnych są na tyle jasne, że nie wymagają ich transpozycji do krajowego porządku prawnego i nadają się do ich bezpośredniego zastosowania. Wyjątek w tym zakresie stanowi nakładanie administracyjnych kar pieniężnych na wskazane w rozporządzeniu *organy i podmioty publiczne.* Wobec sektora publicznego Prezes Urzędu nakładając administracyjna kare pieniężne nie może bowiem zastosować przesłanki wdrożenia bądź nie przez karanego zatwierdzonych kodeksów postępowania na mocy art. 40 rozporządzenia 2016/679 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 rozporządzenia

2016/679. Obie instytucje adresowane są bowiem do przedsiębiorców w tym mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Zastosowanie wskazanych przesłanek w przypadku administracyjnych kar pieniężnych zostało więc wyłączone, w przypadku kar nakładanych na sektor publiczny. Art. 83 ust. 7 rozporządzenia 2016/679 uprawnia również państwa członkowskie do tego, by każde z nich zdecydowało, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim. Jednocześnie, w rozporządzeniu 2016/679 brak jest definicji organów i podmiotów publicznych. Uwzględniając bardzo wysoki wymiar możliwej do nałożenia i przewidzianej w rozporządzeniu 2016/679 kary, wątpliwym jest, czy ich nakładanie na sektor publiczny nie wpłynęłoby na stopień realizacji przez szeroko rozumianą administrację zadań publicznych. Kary nakładane na sektor publiczny nie pełnią również ani roli represyjnej ani prewencyjnej, a ich wpłacanie stanowi często przelewanie środków z tego samego budżetu. Należy jednak również uznać, że w przypadku części z podmiotów publicznych przetwarzanie przez nie danych osobowych stanowi istotę prowadzonej przez nie działalności – i administracyjne kary pieniężne stanowiłyby skuteczny instrument egzekwowania od nich ich ochrony. Uwzględniając powyższe, projektodawca ograniczył więc krąg podmiotów publicznych wobec których możliwe jest nakładanie administracyjnych kar pieniężnych za naruszenia przepisów o ochronie danych osobowych. W pozostałym zakresie w jakim projektowane przepisy przewidują możliwość nałożenia kary pieniężnej na sektor publiczny, wprowadzają znaczne obniżenie maksymalnej granicy możliwej do nałożenia kary, na 100 000 zł. Powyższe rozwiązanie podyktowane jest założeniem, że wymierzany wymiar kary nie powinien skutkować zaprzestaniem a nawet ograniczeniem należytego wykonywanie przez te podmioty powierzonych im zadań publicznych -co w sposób oczywisty naruszałoby interes publiczny. Uwzględniając szczególnie dolegliwy wymiar możliwych do nakładania przez Prezesa Urzędu administracyjnych kar pieniężnych, projektodawca zdecydował się przyznać mu uprawnienie do tego, by na wniosek podmiotu ukaranego odroczyć uiszczenie kary pieniężnej albo rozłożyć ją na raty ze względu na ważny interes wnioskodawcy (art. 53 ust. 1 projektu).

Jak zostało to już wskazane, rozporządzenie 2016/679 w art. 79 wymaga od państw członkowskich wprowadzenia odrębnej drogi dochodzenia roszczeń tytułu naruszenia przepisów o ochronie danych osobowych – poprzez przyznanie uprawnienia do skierowania „skargi" bezpośrednio do sądu z pominięciem organu nadzorczego (Prezesa Urzędu). Projektodawca wprowadził taką możliwość w art. 55 projektu. W szczególności należy wskazać, że w ocenie projektodawcy obowiązku zapewnienia krajowego mechanizmu dochodzenia roszczeń przewidzianego w art. 79 rozporządzenia 2016/679 nie realizuje obowiązujący już dzisiaj art. 24

Kodeksu Cywilnego. Nie każde naruszenie przepisów o ochronie danych osobowych stanowi bowiem naruszenie prawa do prywatności jako dobra osobistego i nie każde naruszenie prawa do prywatności z przyczyn oczywistych stanowi naruszenie ochrony danych osobowych. W ocenie projektodawcy koniecznym było wprowadzenie więc odrębnej podstawy prawnej kierowania do sądów powszechnych (sądów okręgowych) roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych. O ile ani sąd powszechny ani Prezes Urzędu nie powinni być związani swoimi rozstrzygnięciami – w przypadku, gdy skarżący zdecyduje się skorzystać jednocześnie zarówno z drogi sądowej i drogi administracyjno-prawnej, o tyle koniecznym było w ocenie projektodawcy wprowadzenie mechanizmów, zobowiązujących organy do zapoznania się z zapadłym już pierwszym rozstrzygnięciem. Należy bowiem wyeliminować ryzyko pojawienia się sytuacji, gdy Prezes Urzędu bądź sąd powszechny wydadzą wobec siebie sprzeczne rozstrzygnięcia wskutek braku informacji o zapadłym już w danej sprawie rozstrzygnięciu. W związku z powyższym, na podstawie art. 57 projektu ustawy, o wniesieniu do sądu pozwu w sprawach naruszenia ochrony danych osobowych, sąd zawiadamia niezwłocznie Prezesa Urzędu. Jeżeli przed Prezesem Urzędu albo sądem administracyjnym toczy się z kolei postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych albo postępowanie takie zostało zakończone, Prezes Urzędu zawiadamia o tym sąd. W takim przypadku do swobodnej decyzji sądu należało będzie uznanie chociażby zasadności zawieszenia postępowania, celem wydania w pierwszej kolejności rozstrzygnięcia przez Prezesa Urzędu.

Przewidziany w art. 37 ust. 7 rozporządzenia 2016/679 obowiązek zawiadomienia Prezesa Urzędu przez administratora lub podmiot przetwarzający o danych kontaktowych inspektora ochrony danych, jest normą na tyle niejasną, że nie nadaje się do bezpośredniego zastosowania. W świetle powyższego, projektodawca zdecydował się wprowadzić do projektowanej ustawy mechanizmy przekazywania Prezesowi Urzędu rzeczonych informacji wskazując termin ich przekazania, ich treść oraz nakładając obowiązek ich aktualizacji. W ocenie projektodawcy byłoby bardzo cennym, gdyby praktyką było przeprowadzanie takich czynności wyłącznie drogą elektroniczną – co znacznie usprawniłoby zarówno ich doręczanie Prezesowi Urzędu jak i ich otrzymywanie i ewidencjonowanie przez Prezesa. W ocenie projektodawcy nie można jednak dyskryminować podmiotów, które nie mają dostępu do sieci Internet bądź nie wyrażają woli korzystania z systemu teleinformatycznego w przypadku takiej notyfikacji. W takiej sytuacji, powinni oni mieć możliwość przekazywania Prezesowi Urzędu informacji o inspektorach ochrony danych drogą tradycyjną. Rozporządzenie 2016/679 nie zawiera również definicji *organów i podmiotów publicznych* obowiązanych do wyznaczenia inspektora ochrony danych. Projektodawca przyjął więc szerokie rozumienie takiego pojęcia wskazując, że rozumie się przez

nie organy publiczne wskazane w art. 5 § 2 pkt 3 KPA oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Powyższe bez wątpienia wpłynie na zwiększenie poziomu ochrony danych osobowych w sektorze publicznym. Konieczne jest również wprowadzenie przepisu przejściowego, w świetle którego wyjaśniony zostałby status obecnych administratorów bezpieczeństwa informacji w okresie zaraz po rozpoczęciu stosowania rozporządzenia 2016/679. Konieczne jest tutaj z jednej strony poszanowanie interesów administratorów bezpieczeństwa informacji którzy z uwagi na znaczną liczbę dodatkowych obowiązków przewidzianych rozporządzeniem 2016/679 mogą nie chcieć pełnić funkcji jako inspektor ochrony danych, z drugiej strony poszanowanie praw osób których dane osobowe są przetwarzane i chronione przez takich inspektorów. Poszukując rozwiązania kompromisowego, projektodawca zapoznał się z propozycją legislacyjną doręczoną mu przez Generalnego Inspektora Ochrony Danych Osobowych oraz ze stanowiskiem przekazanym mu przez Stowarzyszenie Administratorów Bezpieczeństwa Informacji. W ocenie projektodawcy najwłaściwszym rozwiązaniem, jest przesądzenie wprost, że osoby wykonujące w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, pełnią funkcję inspektora ochrony danych do dnia 1 września 2018 r. Do tego czasu, każdy z inspektorów ochrony danych ma czas na podjęcie decyzji o dalszym pełnieniu takiej funkcji (i dokonaniu stosowanego zawiadomienia do Prezesa Urzędu). W razie braku do tego czasu jakiejkolwiek aktywności z ich strony, w dniu 1 września 2018 r. z mocy prawa przestaną pełnić funkcję inspektorów ochrony danych. Wskazany przepis w ostatecznym projekcie ustawy znajdzie się w rozdziale zawierającym tzw. przepisy przejściowe – podobnie jak chociażby prawna regulacja dotycząca statusu prawnego prowadzonego obecnie przez Generalnego Inspektora rejestru administratorów bezpieczeństwa informacji oraz rejestru zbiorów danych osobowych. Projektodawca zdecydował się jednak na udostepnienie opinii publicznej rzeczonej regulacji dotyczącej administratorów bezpieczeństwa informacji już teraz, z uwagi na jej doniosłe znaczenie jako mającej wpływ na zakres praw i obowiązków takich osób – będących liczną grupą zawodową. Projektodawca jednocześnie zachęca jednak obecnych administratorów bezpieczeństwa informacji, którzy z uwagi na zakres swoich zadań nie chcą pełnić funkcji inspektów ochrony danych, by jeszcze przed 25 maja 2018 r. podjęli wobec administratora danych osobowych bądź podmiotu przetwarzającego decyzję o swojej rezygnacji. W takim przypadku administrator bądź podmiot przetwarzający zobowiązani są powiadomić Generalnego Inspektora o ich odwołaniu.

W ocenie projektodawcy przewidziane w art. 42 rozporządzenia 2016/679 mechanizmy certyfikacji oraz akredytacji wymagają uzupełnienia o aspekty proceduralne. Założeniem przyświecającym w tym zakresie projektodawcy było usprawnienie certyfikacji oraz akredytacji

poprzez ustanowienie jasnych zasad jej przeprowadzania – pozostających jednocześnie w pełnej zgodności z prawem unijnym. Projektowane przepisy przewidują w szczególności treść wniosków akredytacyjnych oraz certyfikacyjnych oraz procedurę podejmowania czynności sprawdzających. Zarówno Prezes Urzędu podczas podejmowania czynności akredytacyjnych (oraz później weryfikując zgodność działań podmiotów certyfikujących z przepisami o ochronie danych) jak i podmioty certyfikujące podejmując czynności zmierzające do przyznania certyfikatu (oraz później weryfikując zgodność działań podmiotów certyfikowanych z przepisami o ochronie danych) muszą mieć instrumenty prawne pozwalające im podejmować takie działania. Powyższe może się wiązać bowiem chociażby z koniecznością wkroczenia w obszar przetwarzania przez dany podmiot danych osobowych. Jednocześnie jednak fakultatywny charakter samej akredytacji i certyfikacji oraz brak władztwa administracyjnego podczas dokonywania samej certyfikacji, w ocenie projektodawcy wyłącza możliwość zastosowania w tych przypadkach przepisów o postępowaniu kontrolnym prowadzonym przez Prezesa Urzędu. Projektodawca zdecydował więc o wprowadzeniu w tym zakresie do tworzonej ustawy przepisów regulujących zasady podejmowania czynności sprawdzających – mniej sformalizowanych. Państwom członkowskim przyznana została również swoboda w podjęciu decyzji, czy Prezes Urzędu będzie wyłącznie akredytował podmioty certyfikujące, czy należy przyznać mu również uprawnienia do samej certyfikacji. W ocenie projektodawcy kompetencje Prezesa Urzędu powinny być ograniczone wyłącznie do akredytacji podmiotów certyfikujących, a certyfikacja należeć powinna do wyspecjalizowanych podmiotów zajmujących się zawodowo ochroną danych osobowych. Przeciwne rozwiązanie polegające na przyznaniu Prezesowi Urzędu również uprawnień certyfikacyjnych stanowiłoby znaczne obciążenie administracyjne dla polskiego organu. Należy również przypuszczać, że przyznanie uprawnień certyfikacyjnych zarówno Prezesowi Urzędu, jak i podmiotom wyspecjalizowanym skutkowałoby tym, że w praktyce większość z administratorów oraz podmiotów przetwarzających korzystałaby z certyfikacji podejmowanej wyłącznie przez Prezesa Urzędu.