**GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH**
*dr Edyta Bielak-Jomaa*

RPW/53436/2017 N
Data:2017-09-11

DESiWM-070-18/17/68794

**Warszawa, dnia 11 ~~sierpnia~~ września 2017 r.**

BIURO RZECZNIKA PRAW OBYWATELSKICH
WPŁ. 2017 -09- 11
ZAŁ. 60 NR

**Pan**
**Adam Bodnar**
**Rzecznik Praw Obywatelskich**

Szanowny Panie Rzeczniku,

w odpowiedzi na pismo z dnia 26 czerwca 2017 r., znak: VII.501.315.2014.AG, chciałabym bardzo podziękować za podjęcie przez Pana Rzecznika tak ważnego problemu, jakim jest właściwe wdrożenie w polskim systemie prawnym unijnej reformy ochrony danych osobowych, w tym przede wszystkim wdrożenie przepisów 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). Obecnie podejmowane działania w tym zakresie będą niewątpliwie determinowały kształt systemu ochrony danych osobowych na kolejne dekady, a co za tym idzie będą miały bezpośredni wpływ na funkcjonowanie konstytucyjnych gwarancji autonomii informacyjnej jednostki w Polsce.

Z tego względu Generalny Inspektor Ochrony Danych Osobowych – jako niezależny i wyspecjalizowany organ nadzorczy ds. ochrony danych osobowych – już od rozpoczęcia prac legislacyjnych na forum UE aktywnie podejmował działania zmierzające do zapewnienia spójności przyszłego systemu ochrony danych osobowych oraz przeciwdziałania próbom obniżania poziomu ochrony danych osobowych w stosunku do dotychczasowych standardów. Generalny Inspektor od 2012 r. zarówno inicjował dyskusje i debaty z udziałem szeregu interesariuszy, jak i merytorycznie wspierał w samym procesie legislacyjnym Rząd RP oraz biorących w nim udział polskich posłów do Parlamentu Europejskiego. Równie proaktywne podejście Generalny Inspektor prezentował po formalnym przyjęciu pakietu legislacyjnego przez UE w 2016 r., czego przejawem było wielokrotne oferowanie Ministerstwu Cyfryzacji merytorycznego wsparcia w procesie wdrożenia



*ul. Stawki 2, 00-193 Warszawa*
*tel. 22 531-03-88*
*fax 22 531-03-99*
www.giodo.gov.pl
@GIODO_GOV_PL

ogólnego rozporządzenia o ochronie danych, co jest o tyle istotne, że choć Generalny Inspektor ma największą wiedzę i doświadczenie w tej materii, to jednak nie przysługuje mu inicjatywa legislacyjna.

Proces wdrożenia ogólnego rozporządzenia o ochronie danych musi uwzględniać charakter prawny tego aktu prawnego. Otóż zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej, rozporządzenie ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Oznacza to, że większość przepisów ogólnego rozporządzenia o ochronie danych będzie stosować się bezpośrednio we wszystkich państwach członkowskich, co więcej nie może być w żaden sposób implementowana do prawa krajowego, ani nawet interpretowana przez ustawodawcę krajowego. Jedynie motyw 8 preambuły ogólnego rozporządzenia o ochronie danych wskazuje, że w zakresie, w jakim to rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy rozporządzenia do swego prawa krajowego. Oznacza to, że zasadnicza część regulacji ochrony danych osobowych została zawarta w ogólnym rozporządzeniu o ochronie danych, a pozostawiono jedynie pewien zakres materii podlegających regulacji krajowej. W tym kontekście podkreślenia wymaga, że polski ustawodawca powinien przede wszystkim skoncentrować się na przyjęciu tych przepisów, bez których nie byłoby możliwe właściwe stosowanie rozporządzenia 2016/679.

Niewątpliwie do tej materii należy określenie pozycji ustrojowej i kompetencji organu nadzorczego. Jednakże rozporządzenie 2016/679 wprowadzając nowy system ochrony danych osobowych nie kształtuje go w próżni, lecz opiera go na dotychczasowych rozwiązaniach instytucjonalnych, poddając je jedynie niezbędnym modyfikacjom. Rozporządzenie 2016/679 nie tworzy zupełnie nowych instytucji określanych mianem „organów nadzorczych", lecz ujednolica status i kompetencje oraz gwarancje niezależności istniejących już od wielu lat w państwach członkowskich UE organów nadzorczych. Oznacza to, że ustawodawca krajowy musi zapewnić prawną i faktyczną ciągłość działania tych organów. Nie może wiec dopuścić do sytuacji braku lub ograniczenia instytucjonalnych gwarancji ochrony danych osobowych w państwie członkowskim UE. Gwarancje te obejmują również kwestie niezależności organów nadzorczych, które zostały wyraźnie potwierdzone przez Trybunał Sprawiedliwości UE. Z tego względu wszelkie zmiany instytucjonalne wprowadzane w ramach procesu wdrożenia rozporządzenia 2016/679 muszą spełniać wysokie standardy dotyczące niezależności organów nadzorczych, co m.in. oznacza zakaz skrócenia *de iure*, czy też *de facto* kadencji istniejących dotąd organów ochrony danych osobowych.

Właściwe wdrożenie rozporządzenia 2016/679 nie może się ograniczać do jedynie do działań legislacyjnych. Dużą rolę w powodzeniu tego procesu odgrywają bowiem organy nadzorcze na poziomie krajowym, jak i unijnym. Ustawodawca europejski przewidział szerokie kompetencje opiniodawcze Europejskiej Rady Ochrony Danych, która zastąpi obecną Grupę Roboczą Art. 29 ds. ochrony danych osobowych. Dlatego Grupa Robocza Art. 29 opracowuje wytyczne poświecone różnym aspektom stosowania przepisów rozporządzenia 2016/679, które zostaną przyjęte przez Europejską Radę Ochrony Danych zgodnie z jej nowymi kompetencjami po 25 maja 2018 r., a obecnie umożliwiają administratorom danych i podmiotom przetwarzającym przygotowanie się do przestrzegania nowych przepisów o ochronie danych osobowych. Również krajowe organy nadzorcze, w tym Generalny Inspektor podejmują liczne działania mające na celu zapewnienie właściwego wdrożenia rozporządzenia 2016/679.

Generalny Inspektor w dniu 8 lipca 2016 r. powołał w drodze zarządzenia w ramach Biura GIODO Zespół roboczy do spraw reformy przepisów o ochronie danych osobowych w Unii Europejskiej, którego zadaniem jest prowadzenie wewnętrznych działań, w tym przygotowywanie analiz, związanych z przyjęciem rozporządzenia 2016/679.

W toku prac Zespołu został opracowany dokument zawierający wstępne uwagi Generalnego Inspektora dotyczące zakresu i kształtu przyszłych przepisów wdrażających rozporządzenie 2016/679 w odniesieniu do statusu i kompetencji organu ochrony danych oraz aspektów proceduralnych nowych przepisów o ochronie danych osobowych. Dokument został przekazany Ministrowi Cyfryzacji oraz udostępniony na stronie internetowej Biura GIODO, a jego kopię załączam do pisma. Jednocześnie Zespół roboczy rozpoczął prace nad projektem przepisów, które mogłyby znaleźć się w przygotowywanym przez Ministra Cyfryzacji projekcie nowej ustawy o ochronie danych osobowych. W dniu 27 stycznia 2017 r. wstępna propozycja przepisów dotyczących postępowania przed organem nadzorczym została przedstawiona Ministrowi Cyfryzacji. Z przykrością informuję, że oba ww. dokumenty nie spotkały się z żadną formalną odpowiedzią ze strony Ministra Cyfryzacji.

Generalny Inspektor w piśmie z dnia 17 lipca 2017 r., które przekazuję w załączeniu, odnosząc się do prośby Ministra Cyfryzacji dotyczącej przygotowania - w oparciu o przepisy ogólnego rozporządzenia o ochronie danych oraz przesłanej przez Ministra Cyfryzacji części projektu przepisów ustawy i założeń oceny skutków regulacji przyszłych rozwiązań prawnych - wyliczenia kosztów funkcjonowania przyszłego organu ochorny danych osobowych, należy wskazać, że przekazane w tym zakresie informacje były niewystarczące do przedstawienia żądanych wyliczeń. Znajomość jedynie części założeń funkcjonowania przyszłego organu ochrony danych oobowych uniemozliwia podanie prawidłowych/racjonalnych kosztów jego funkcjonowania. Przekazane dokumenty, oprócz wskazania nowej nazwy organu, nie rozstrzygają

kwestii dotyczących statusu organu. Generalny Inspektor nie otrzymał żadnych informacji dotyczących sposobu „powstania" Urzędu Ochrony Danych Osobowych. Ponadto, w założeniach ustrojowej części przepisów projektowanej ustawy o ochronie danych osobowych wskazano na szereg zmian w stosunku do obecnego kształtu organu ochrony danych. Należy zauważyć, że ta najistotniejsza, z punktu widzenia funkcjonowania organu kwestia nie znalazła wyrazu w propozycji konkretnych przepisów.

Ponadto, w dniu 28 lipca 2017 r. do Ministra Cyfryzacji zostało skierowane pismo zawierające uwagi do przekazanego w dniu 9 czerwca 2017 r. roboczego projektu ustawy o ochronie danych osobowych, którego kopia stanowi załącznik do niniejszego pisma. Do dnia dzisiejszego Generalny Inspektor nie uzyskał stanowiska Ministra Cyfryzacji do zaprezentowanych na kilkunastu stronach uwag i propozycji. Minister Cyfryzacji w swoim piśmie skierowanym do Rzecznika Praw Obywatelskich wskazał, że „informacja prasowa wskazująca, że Generalny Inspektor został odsunięty od prac nad ustawą jest nieprawdziwa". Pozwolę sobie nie zgodzić się z tym stwierdzeniem. Należy wskazać, że przedstawionej w piśmie Ministra Cyfryzacji współpracy nie można nazwać dialogiem nad wspólnym wypracowaniem projektu ustawy o ochronie danych osobowych a jednostronnym przedstawianiem własnej wizji nowego systemu ochrony danych osobowych w Polsce. Poważne obawy Generalnego Inspektora budzi fakt, że przy tworzeniu w Ministerstwie Cyfryzacji przepisów nie bierze się pod uwagę dotychczasowego doświadczenia organu ochrony danych osobowych oraz bagatelizuje się problemy, na które zwraca uwagę Generalny Inspektor.

Mimo wielokrotnych zapewnień składanych w mediach przez Ministra Cyfryzacji oraz jego przedstawicieli, o tym że projekt ustawy o ochronie danych osobowych zostanie udostępniony do uzgodnień, konsultacji oraz opiniowania do końca pierwszego kwartału 2017 r., następnie w czasie wakacji - projekt ustawy dopiero pod koniec sierpnia 2017 r. został wpisany do Wykazu prac legislacyjnych i programowych Rady Ministrów. Udostępniony Generalnemu Inspektorowi roboczy projekt przepisów ustawy o ochronie danych osobowych z dnia 9 czerwca 2017 r. w kwestii przepisów regulujących funkcjonowanie organu nadzorczego zawierał komentarz o uzgadnianiu treści tych przepisów. Tak więc najistotniejsze z punktu widzenia przyszłości niezależnego organu do spraw ochrony danych osobowych regulacje nie zostały przedstawione do dnia dzisiejszego Generalnemu Inspektorowi. Wydaje się, że Minister Cyfryzacji zapewniając o prowadzonej współpracy miał na myśli jedynie selektywne uzgadnianie przepisów projektowanej ustawy o ochronie danych osobowych. Należy przewidywać, że zaprezentowanie najważniejszych względem Generalnego Inspektora Ochrony Danych przepisów nastąpi dopiero w momencie skierowania ostatecznej wersji projektu do zaopiniowania.

Wątpliwości budzi również fakt, czy skoro Minister Cyfryzacji mając świadomość „napiętego kalendarza legislacyjnego, który obejmuje zmianę ustawy o ochronie danych osobowych oraz setek przepisów sektorowych" i podejmując się samodzielnego projektowania ustawy będzie w stanie wywiązać się z ciążącego na nim obowiązku zapewnienia stosowania rozporządzenia 2016/679 w terminie. Generalny Inspektor nieustannie deklaruje chęć pomocy i współpracy przy stworzeniu przepisów nowej ustawy o ochronie danych osobowych. Należy pamiętać, że dołożenie należytej staranności przy opracowaniu tego projektu aktu prawnego będzie miało wpływ na realizację prawa podstawowego jakim jest prawo do ochrony danych osobowych.

Właściwe wdrożenie rozporządzenia 2016/679 wymaga szerokiej debaty publicznej oraz działań zwiększających świadomość społeczną. Z tego względu ostatnie miesiące to również czas intensywnych konferencji, szkoleń i spotkań poświęconych reformie ochrony danych osobowych. Należy bowiem podkreślić, że Generalny Inspektor na podstawie art. 12 ust. 5 ustawy o ochronie danych osobowych jest obowiązany do inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych. Do takich przedsięwzięć należy zaliczyć organizację licznych konferencji o wykonywaniu funkcji inspektora ochrony danych, szkoleń dla ABI z różnych sektorów branżowych oraz udział ekspertów GIODO w wielu panelach dyskusyjnych oraz konferencjach organizowanych przez inne podmioty.

Konferencją, której jednym z głównych tematów było przygotowanie do rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych osobowych była konferencja w dniu 31 stycznia 2017 r. pn.: „Ochrona danych osobowych w dobie przemian". Podczas swojego wystąpienia na konferencji Sekretarz Stanu w Ministerstwie Cyfryzacji – Pan Marek Zagórski ogólnie odniósł się do planowanych zmian instytucjonalnych. Ponadto podczas wystąpienia w panelu dyskusyjnym przedstawiciela Ministerstwa Cyfryzacji została zaprezentowana m.in. idea powołania przy organie nadzorczym Rady ds. Ochrony Danych (jako wzór wskazano funkcjonujące w organach administracji rządowej ciała doradcze), uprawnienie do samodzielnego nadawania statutu oraz konieczność związania pracowników Biura tajemnicą zawodową.

Niestety Minister Cyfryzacji nie przyjął zaproszenia na organizowaną przy okazji spotkania organów ochrony danych z państw Grupy Wyszehradzkiej przez Generalnego Inspektora konferencji połączonej z posiedzeniem Komisji Praw Człowieka, Praworządności i Petycji Senatu RP na temat przyszłości organu ochrony danych. Do grona dyskutantów zaproszeni zostali przedstawiciele środowiska naukowego, biznesu, organizacji pozarządowych, a także reprezentanci organów ochrony danych z państw Grupy Wyszehradzkiej.

Przykładem zainicjowania przez Generalnego Inspektora debaty publicznej było zorganizowanie wspólnie z Rzecznikiem Praw Dziecka w dniu 9 lutego 2017 r. seminarium eksperckiego dotyczącego swobody regulacyjnej w zakresie ustalenia granicy wieku, od którego dziecko może samodzielnie wyrazić zgodę na przetwarzanie danych osobowych w związku z korzystaniem z usług społeczeństwa informacyjnego. W spotkaniu uczestniczyli eksperci z różnych dziedzin i osoby reprezentujące różne urzędy, w tym Ministerstwo Edukacji Narodowej, Ministerstwo Cyfryzacji i Krajową Radę Radiofonii i Telewizji. Uczestniczący w spotkaniu prelegencji wskazali na konieczność pogłębionej analizy tego zagadnienia i poddanie tego tematu szerokim konsultacjom. Przedstawiciel Ministra Cyfryzacji podczas swojej prezentacji przedstawił stanowisko Ministra Cyfryzacji o obniżeniu w Polsce tego wieku do lat 13. Generalny Insektor chcąc kontynuuować rozpoczętą dyskusję na ten temat zaprosił do wyrażenia swojej opinii w tym temacie pedagodów ze szkół uczestniczących w programie „Twoje dane- Twoja sprawa". Wyniki tych konsultacji zostały udostępnione na stronie Generalego Inspektora Ochroy Danych Osobowych.

Przedstawione powyżej wydarzenia to tylko niektóre z działań podjętych przez krajowy organ ochrony danych, które mają na celu dyskusję i wymianę doświadczeń związanych z kwestią ochrony danych i zbliżającymi się zmianami. Do udziału w takich spotkaniach zapraszane jest szerokie grono osób, których dotychczasowa praktyka w zakresie ochrony danych osobowych może posłużyć do odpowiedniego przygotowania się do stosowania rozporządzenia 2016/679.

Warto również wspomnieć, że Generalny Inspektor współpracuje również z administratorami bezpieczeństwa informacji, profesorami oraz specjalistami z różnych dziedzin w ramach powołanej Komisji Ekspertów do spraw reformy prawa ochrony danych osobowych w Unii Europejskiej. Przedmiotem prac są zagadnienia istotne w kontekście prac nad krajowymi regulacjami, m.in. przepisy ustrojowe regulujące funkcjonowanie Generalnego Inspektora Ochrony Danych Osobowych (GIODO) od 25 maja 2018 r., ustanawianie sektorowych ograniczeń stosowania rozporządzenia na podstawie jego art. 23 oraz tworzenie odrębnych regulacji zasad przetwarzania danych osobowych przez kościoły i związki wyznaniowe. Dyskusji poddawane są również wstępne projekty przepisów ustawy o ochronie danych osobowych zaprezentowane przez Ministerstwo Cyfryzacji.

Biorąc pod uwagę obecny stan prac nad przepisami wdrażającymi w polskim porządku prawnym ogólne rozporządzenie o ochronie danych, Generalny Inspektor Ochrony Danych Osobowych wyraża poważne obawy, czy w terminie określonym przez prawodawcę unijnego zostaną przyjęte wszystkie niezbędne w tym zakresie przepisy prawa.

Z wyrazami szacunku

Stempel

GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH
Edyta Bielak- Jomaa

Warszawa, dnia 28 lipca 2017 r.

Pani
Anna Streżyńska
Minister Cyfryzacji

w nawiązaniu do przekazanego projektu ustawy o ochronie danych osobowych z dnia 19 maja 2017 r., poniżej przedstawiam uwagi Generalnego Inspektora Ochrony Danych Osobowych do przedmiotowego projektu.

Na wstępie należy zauważyć, że przedstawiona propozycja projektu ustawy nie zawiera kompletnych regulacji dotyczących przyszłości systemu ochrony danych osobowych w Polsce. Dla pełnej oceny zaproponowanych przez Ministra Cyfryzacji rozwiązań niezbędna jest analiza, brakujących w tym projekcie, przepisów ustrojowych regulujących niezależność organu, przepisów dotyczących zmian w poszczególnych sektorach oraz podstawowych regulacji dotyczących określenia przedmiotu i zakresu ustawy.

**1. Systematyka projektu ustawy**- Zasadne wydaje się rozważenie zmiany kolejności rozdziałów projektu ustawy. W ocenie Generalnego Inspektora zasadne byłoby umieszczenie rozdziału dotyczącego Prezesa Urzędu Ochrony Danych Osobowych przed rozdziałem 2 i 3 projektu. W przypadku uwzględnienia tej uwagi należy odpowiednio przeredagować art. 1 ust. 2 projektu.

**2. Wyłączenie stosowania rozporządzenia 2016/679 w zakresie Prawa prasowego (art. 2)**- W art. 85 ust. 1 rozporządzenia 2016/679 posłużono się pojęciem „przetwarzania dla potrzeb dziennikarskich", co oznacza działania w zakresie szerszym, aniżeli tylko tworzenie oraz publikowanie materiałów prasowych. Zauważyć należy, że przyjęcie rozwiązania zaproponowanego w art. 2 ust. 1 projektu mogłoby w istocie prowadzić do fikcyjności powyższego wyjątku. Trudno bowiem przyjąć racjonalność sytuacji, w której co prawda przepisy rozporządzenia 2016/679 nie ograniczają możliwości wytworzenia materiału prasowego, jednakże stoją na przeszkodzie zebraniu materiałów mających być podstawą do stworzenia tegoż materiału prasowego.

W rozporządzeniu 2016/679 (art. 85 ust. 1) posłużono się sformułowaniem „wypowiedź artystyczna, literacka". Zastąpienie tego sformułowania pojęciem „działalność" mogłoby prowadzić



ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

do nieuzasadnionego zawężenia wyłączenia. W potocznym języku polskim pojęcie „działalność" jest bowiem rozumiane jako czynności powtarzające się, czy wręcz ciągłe. Tymczasem ochroną wynikająca z prawa do wolności słowa powinny być także objęte pojedyncze wypowiedzi, wystąpienia, apele.

W kontekście brzmienia art. 85 ust. 1 rozporządzenia 2016/679 wątpliwości budzi zaproponowane wyłączenie stosowania niektórych przepisów rozporządzenia do „działalności akademickiej", w sytuacji, gdy w akcie unijnym mowa jest o „wypowiedzi akademickiej". Pojęcia te nie są tożsame, ponieważ działalność akademicką należy rozumieć szerzej jako kształcenie studentów i prowadzenie badań naukowych, nie zaś jako poszczególne wykłady, referaty, artykuły.

Rozważenia wymaga również, zbyt szeroki zakres zaproponowanego wyłączenia przepisów.

**3. Ustalenie granicy wieku, w jakim dziecko samodzielnie może wyrazić zgodę na przetwarzanie danych w przypadku usług świadczonych drogą elektroniczną (art. 3)**- Generalny Inspektor zainicjował szerszą dyskusję w kwestii granicy wieku, w jakim dziecko samodzielnie może wyrazić zgodę na przetwarzanie danych w przypadku usług świadczonych drogą elektroniczną. W dniu 9 lutego 2017 r. zostało zorganizowane wraz z Rzecznikiem Praw Dziecka seminarium eksperckie „Zgoda dziecka na przetwarzanie danych osobowych w świetle ogólnego rozporządzenia o ochronie danych". Przedstawiciele Ministerstwa Cyfryzacji również wzięli udział w ww. seminarium. GIODO podjął również dialog ze środowiskiem nauczycieli. Przeprowadzone z tym środowiskiem konsultacje z pozwoliły m.in. stwierdzić, że większość przedstawicieli oświaty opowiada się za zachowaniem granicy wieku określonej w rozporządzeniu 2016/679 (16 lat) bądź niższej o rok (15 lat). Wyniki tych konsultacji są ogólnodostępne na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.

Odnosząc się do zaproponowanego przez Ministerstwo Cyfryzacji w art. 3 projektu wieku dziecka, należy mieć na względzie, że zgodnie z przepisami ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2017 r. poz. 459), 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. Trudno jednak porównywać skutki decyzji podjętej przez taką osobę w drobnych sprawach życia codziennego ze skutkami jakie może nieść ze sobą założenie konta na portalu społecznościowym. W opinii Generalnego Inspektora jest to poważne zagrożenie, tym bardziej, że psychologowie już teraz alarmują, że człowiek buduje poczucie własnej wartości m.in. poprzez wystawianie swojego wizerunku na widok publiczny. Potrzeba uzyskiwania publicznej aprobaty jest na tyle uzależniająca, że specjaliści klasyfikują taki syndrom (*Facebook Addiction Disorder*) na równi z takimi nałogami jak alkoholizm, uzależnienie od narkotyków czy hazardu. Dziecko, które z wiekiem dąży do większej samodzielności, posiadając już własny smartfon, nie mając świadomości skutków swoich działań stoi przed pokusą ujawniania swojej prywatności i danych zaliczających się do szczególnej kategorii, które raz umieszczone w Internecie mogą przynieść negatywne konsekwencje w przyszłości. Należy wziąć też pod uwagę, że wszelkie konsekwencje decyzji dziecka w tej sprawie- zgodnie z obowiązującymi przepisami prawa- ponosić będą jego rodzice bądź przedstawiciele ustawowi.

Jednocześnie należy zauważyć, że z 28 państw członkowskich, które od 25 maja 2018 r. będą stosowały rozporządzenie 2016/679, tylko 4 (w tym Polska) zaproponowały w swoich krajowych przepisach obniżenie wieku dziecka. Większość państw jeszcze nie podjęła tej decyzji

i nie zaproponowała jednoznacznie w projektowanych aktach, czy skorzysta z uprawnienia jakie daje im rozporządzenie 2016/679 i zdecyduje się na obniżenie tego wieku. (źródło: artukuł MLex Market Insight z 7 lipca 2017 r.)

Uwagi wymaga również, że temat ten należy koniecznie poddać szerszej dyskusji z uwzględnieniem chociażby sposobu w jaki administrator strony internetowej mógłby zweryfikować wiek dziecka i sposobu w jaki powinien uzyskiwać zgodę opiekuna prawnego dziecka jeśli nie spełnia ono ustawowej granicy wieku.

Generalny Inspektor ma świadomość tego, że gotowy projekt ustawy, w ramach procesu legislacyjnego, zostanie poddany konsultacjom publicznym i opiniowaniu. Jednak, mając na uwadze określony czas, w jakim podmioty zainteresowane będą mogły zgłaszać swoje uwagi do tego przepisu, należy zauważyć, że ten czas może nie być wystarczający aby w pełni pochylić się na zagadnieniem.

**4. Warunki wyrażenia zgody przez dziecko(art. 3)**- Art. 3 projektu przewiduje, iż przetwarzanie danych możliwe jest wyłącznie po uzyskaniu uprzedniej zgody rodziców lub opiekunów prawnych. Zauważyć należy, że art. 8 ust. 1 rozporządzenia 2016/679 stanowi, że przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała działanie dziecka osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz przetwarzanie jest zgodne z prawem wyłącznie w zakresie wyrażonej zgody. Również ust. 2 art. 8 rozporządzenia 2016/679 odwołuje się do wyrażenia lub zaaprobowania zgody. Przepisy rozporządzenia nie precyzują, jak ma wyglądać wyrażenie bądź zaaprobowanie zgody, zweryfikowanie tej zgody, jak również zweryfikowanie wieku dziecka. Projektodawca w art. 3 nie odniósł się do tej kwestii.

Ponadto należy zauważyć, że art. 8 ust. 1 rozporządzenia 2016/679 posługuje się bardziej precyzyjnym sformułowaniem: „osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem" niż zaproponowany przez projektodawcę: „rodzice lub opiekunowie prawni".

Przeanalizowania wymaga również posłużenie się w omawianym przepisie pojęciem „usług świadczonych drogą elektroniczną". Rozporządzenie 2016/679 posługuje się pojęciem „usług społeczeństwa informacyjnego", które na gruncie krajowych przepisów prawa nie zostało do tej pory zdefiniowane. Co prawda ustawa z dnia 18 lipca 2002 r. o usługach świadczonych drogą elektroniczną (Dz. U. z 2017 r. poz. 1219) posługuje się pojęciem „usług świadczonych droga elektroniczną" ale czy projektodawca zweryfikował wzajemny zakres tego pojęcia z pojęciem „usług społeczeństwa informacyjnego" z rozporządzenia 2016/679?

**5. Inspektorzy ochrony danych**- W wytycznych przygotowanych przez Generalnego Inspektora wskazano, że zgłoszenie danych inspektora do organu nadzorczego nie przewiduje konieczności prowadzenia przez GIODO rejestru. Należy raczej uznać, że organ ochrony danych w takich sytuacjach będzie prowadził wewnętrzną ewidencję o charakterze pomocniczym. W projektowanym art. 4 ust. 5 Minister Cyfryzacji wskazał, że Prezes Urzędu prowadzi ewidencję takich zawiadomień, nie wskazując jaki charakter będzie miało prowadzenie tej ewidencji. Istnieje obawa, że przepis ten będzie odczytywany jako obowiązek prowadzenia jawnej ewidencji, tak jak obecnie prowadzony jest rejestr administratorów bezpieczeństwa informacji.

Należy zwrócić również uwagę na określony w art. 4 ust. 1 katalog danych, które administrator danych lub podmiot przetwarzający będzie obowiązany przekazać organowi nadzorczemu- imię

i nazwisko, adres poczty elektronicznej albo numer telefonu inspektora w kontekście skuteczności ewentualnej weryfikacji prawdziwości przekazanych danych.

Generalny Inspektor proponuje aby zawiadomienia, o których mowa w art. 4 ust. 4 były dokonywane wyłącznie w formie elektronicznej za pośrednictwem systemu, o którym mowa w ust. 6. Natomiast w celu eliminowania fikcyjnych zgłoszeń, zgłoszenia powinny być opatrzone podpisem elektronicznym lub potwierdzonym profilem zaufanym elektronicznej Platformy Usług Administracji Publicznej (ePUAP). Weryfikacja, czy dane zostały przekazane przez osobę uprawnioną do działania w imieniu administratora lub podmiotu przetwarzającego powinna leżeć po stronie wymienionych podmiotów. Takie rozwiązanie będzie możliwe z uwagi na to, że obowiązek dotyczy administratorów i podmiotów przetwarzających, a zatem podmiotów z reguły dysponujących środkami komunikacji elektronicznej, co więcej bardzo często zobowiązanych na mocy innych ustaw do posługiwania się taką formą komunikacji. Ponadto, zawiadomienia papierowe wymagają ręcznego wprowadzania zawartych w nich danych do ewidencji, co jest niepotrzebnym obciążeniem administracyjnym.

W zakresie przepisów dotyczących obowiązku powiadamiania o danych kontaktowych inspektora zastrzeżenia budzi również brak odniesienia się projektodawcy do możliwości powołania jednego inspektora ochrony danych dla kilku podmiotów. W przypadku podmiotów prywatnych, jednego inspektora może powołać grupa przedsiębiorstw (art. 37 ust. 2 rozporządzenia 2016/679). Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych (art. 37 ust. 3 rozporządzenia 2016/679). W związku z powyższym wydaje się, że w projekcie powinny znaleźć się przepisy przewidujące, że w przypadku skorzystania przez administratora lub podmiot przetwarzający z uprawnienia określonego w art. 37 ust. 2-4 rozporządzenia 2016/679, do powiadomienia o danych kontaktowych inspektora ochrony danych zobowiązany jest każdy administrator lub podmiot przetwarzający.

Ponadto projektowane przepisy nie przewidują regulacji w odniesieniu do sytuacji, w której administrator lub podmiot przetwarzający odwoła inspektora ochrony danych i w jego miejsce nie powoła żadnej innej osoby (chodzi o przypadki, w których wyznaczenie inspektora ochrony danych nie jest obowiązkowe). Należy w sposób wyraźny zobowiązać administratorów danych do powiadamiania organu nadzorczego nie tylko do informowania o każdej zmianie danych, ale też o anulowaniu danych kontaktowych inspektora.

W ocenie Generalnego Inspektora w celu zapewnienia prawidłowego i rzetelnego wykonywania funkcji przez inspektorów ochrony danych w projekcie ustawy należy dookreślić wynikający bezpośrednio z art. 38 ust. 5 rozporządzenia 2016/679 obowiązek inspektora ochrony danych do zachowania tajemnicy lub poufności co do wykonywania swoich zadań. Przepisy ustawy krajowej powinny wskazywać przypadki, w których inspektor ochrony danych jest zwolniony z obowiązku zachowania tajemnicy, np. jeżeli informacji objętych tajemnicą zażąda organ nadzorczy - w związku z monitorowaniem stosowania rozporządzenia 2016/679, sąd lub prokurator - w związku z toczącym się postępowaniem lub inne upoważnione organy - w związku z prowadzonym przez te organy postępowaniem. Zasadne jest również zobowiązanie inspektora ochrony danych do zachowania tajemnicy po ustaniu stosunku pracy, stosunku zlecenia lub

w innego stosunku prawnego o podobnym charakterze oraz określenie zasad odpowiedzialności za niedochowanie przedmiotowego obowiązku.

6. **Akredytacja i certyfikacja**- W art. 6 ust 1 projektu zaproponowano aby akredytacji, o której mowa w art. 43 rozporządzenia 2016/679 udzielał krajowy organ nadzorczy, co w opinii Generalnego Inspektora jest jak najbardziej możliwe i byłoby korzystne z punktu widzenia prestiżu i pozycji Biura, ale wydaje się nieuzasadnione ekonomicznie. Wobec tego zdaniem Generalnego Inspektora należy rozważyć wskazanie krajowej jednostki akredytującej jako właściwej dla tych czynności. Spowodowane jest to potrzebą zapewnienia dość rygorystycznych procedur dotyczących zapewnienia transparentności i niezależności tego procesu, w tym zapewnienia, aby poszczególne etapy procesu, takie jak weryfikacja warunków, audyt akredytacyjny, ocena wyników i ich zatwierdzenie dokonywane było przez inne osoby. W opinii Generalnego Inspektora obszar tematyczny procesów poddawanych certyfikacji wynikający z rozporządzenia 2016/679 jest najbardziej zbliżony do akredytacji dotyczącej systemów zarządzania bezpieczeństwem informacji, którą przeprowadza Polskie Centrum Akredytacyjne (PCA). Wymagania akredytacyjne PCA dla podmiotów certyfikujących systemy zarządzania bezpieczeństwem informacji bazują na normach:

- PN-EN ISO/IEC 17021-1 Ocena zgodności. Wymagania dla jednostek prowadzących audyty i certyfikację systemów zarządzania Część 1: Wymagania,
- ISO/IEC 27006 Technika informatyczna - Techniki bezpieczeństwa - Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji.

Z informacji zamieszczonych na stronie internetowej PCA (www.pca.gov.pl) wynika, że akredytację w odniesieniu do normy PN-EN ISO/IEC 17021 w zakresie zarządzania systemami bezpieczeństwa informacji posiada obecnie tylko 7 firm.

Biorąc pod uwagę powyższe można szacować, że również w zakresie certyfikacji na zgodność z rozporządzeniem 2016/679 zgłosi się z wnioskiem o akredytację nie więcej niż ok. 7 podmiotów. Ponadto, biorąc pod uwagę przedział czasowy składanych w tym przedmiocie wniosków o uzyskanie akredytacji, np. od 0 do 5 podmiotów w pierwszym roku i od 0-2 w następnych latach, nieuzasadnione wydaje się powielanie sprawnie działającej w PCA infrastruktury akredytacyjnej w organie nadzorczym. Konieczność zapewnienia transparentności i bezstronności procesu akredytacyjnego wymaga zapewnienia w tym obszarze określonych standardów, jak np. zapewnienie, aby osoba oceniająca wniosek akredytacyjny nie była jednocześnie osobą, która dokonuje audytu akredytacyjnego ani osobą zatwierdzającą jego wyniki.

Należy również brać pod uwagę, że jednostka organu nadzorczego odpowiedzialna za przeprowadzanie kontroli nie powinna przeprowadzać akredytacji ani certyfikacji. Dział kontroli i dział akredytacji/ certyfikacji mają inne obszary działania, a ich powiązanie mogłoby być czynnikiem korupcjogennym. Należy pamiętać o tym, że polityka bezstronności to jedna z głównych polityk wynikająca z norm dotyczących oceny zgodności.

Zaproponowana przez Ministra Cyfryzacji koncepcja będzie wiązała się z dodatkowymi kosztami. Do kosztów związanych z utworzeniem w organie nadzorczym niezależnej od PCA jednostki akredytacyjnej należałoby zaliczyć w szczególności:

- powołanie nowego zespołu ekspertów,
- opracowanie polityk i procedur związanych z procesem akredytacji,

- opracowanie wzorców dokumentów,
- opracowanie narzędzi audytowych,
- zaprojektowanie znaku jakości (nadania akredytacji) oraz jego zgłoszenie w Urzędzie Patentowym w celu uzyskania świadectwa ochronnego.

W związku z powyższym, zasadnym modelem byłoby wskazanie PCA jako jednostki akredytującej, która zobowiązana byłaby do współpracy z organem nadzorczym w zakresie oceny, np. poprzez udział przedstawicieli organu nadzoru w istniejącej w PCA Radzie ds. Akredytacji oraz w opracowaniu kryteriów akredytacyjnych.

Ministerstwo Cyfryzacji posługuje się w projekcie pojęciem „wnioskodawcy". Należy zauważyć, że rozporządzenie 2016/679 nie posługuje się takim pojęciem. Generalny Inspektor ma świadomość tego, że w sytuacji gdy podmiot jeszcze nie uzyskał akredytacji nie powinno się go nazywać podmiotem akredytowanym, ale posługiwanie się pojęciem wnioskodawcy w tym miejscu może budzić wątpliwości.

Należy również zasygnalizować, że w przepisach ogólnych trzeba określić, za pomocą jakich środków organ będzie komunikował się z „petentami". Rozporządzenie 2016/679 niejednokrotnie wskazuje, że pożądane jest prowadzenie korespondencji w postaci elektronicznej. Dotyczy to szczególnie kwestii związanych z prowadzeniem korespondencji za pomocą e-maila, identyfikacją petentów i ich weryfikacją, zabezpieczeniem przekazywanych danych, wymogiem podpisywania dokumentów itd. Wydaje się, że Ministerstwo Cyfryzacji, jako organ odpowiedzialny za informatyzację administracji publicznej, powinno zaproponować wyczerpujące rozwiązania w tym zakresie.

**7. Zawiadomienie o udzieleniu akredytacji (art. 7 ust. 5)** – W ocenie Generalnego Inspektora obowiązek przedstawiony w art. 7 ust. 5 wynika z ogólnego rozporządzenia o ochronie danych osobowych i nie ma potrzeby przenoszenia tego do krajowych przepisów.

Analizując przepisy zaproponowane przez Ministerstwo Cyfryzacji w zakresie akredytacji i certyfikacji nasuwa się skojarzenie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398). Nie sposób w tym miejscu nie zadać pytania, czy skoro uregulowano, jak informuje się „wnioskodawców" o udzieleniu akredytacji to, czy nie należałoby zaproponować przepisów odnoszących się do postępowania w przypadku nieudzielenia akredytacji. Czy Minister Cyfryzacji zastanawiał się nad dopuszczalnością złożenia odwołania w przypadku nieudzielenia akredytacji? Jakie uprawnienia będą przysługiwały niezadowolonemu „wnioskodawcy"? W szczególności należy zadać pytanie, według jakich zasad będzie prowadzone to postępowanie? Czy zastosowanie będą tu miały przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257)?

W art. 7 ust. 4 projektu wskazano, że Prezes Urzędu rozpatruje wniosek o akredytację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia kompletnego wniosku zawiadamia wnioskodawcę o udzieleniu lub odmowie udzielenia akredytacji. W opinii Generalnego Inspektora zaproponowany termin 3 miesięcy należałoby wydłużyć do co najmniej 6 miesięcy, gdyż proces akredytacji obejmuje wiele działań, w szczególności dotyczy weryfikacji podmiotu ubiegającego się o akredytację w zakresie:

- struktury organizacyjnej i dokumentów organizacyjnych,

- kompetencji personelu,
- dokumentów dotyczących procesu certyfikacji,
- dokumentów z przeprowadzonych certyfikacji,
- zasad zachowania bezpieczeństwa informacji,

poprzez weryfikację dokumentów, jak również wykonanie audytów na miejscu. W przypadku akredytacji podmiotów wielooddziałowych wymaga to przeprowadzenia dodatkowych audytów. Biorąc to pod uwagę, przeprowadzenie akredytacji w terminie maksymalnym 3 miesięcy może być w przypadku dużych, wielooddziałowych organizacji niewykonalne. Posługując się porównaniem- w art. 23 ust. 5 ustawy o systemach oceny zgodności i nadzoru rynku, Polskie Centrum Akredytacji rozpatruje wniosek o udzielenie akredytacji i w terminie nie dłuższym niż 12 miesięcy od dnia złożenia kompletnego wniosku zawiadamia wnioskującą jednostkę o udzieleniu albo odmowie udzielenia akredytacji.

**8. Certyfikat**- w art. 8 ust. 1 projektu ustawy projektodawca wskazuje, że „dokumentem potwierdzającym akredytację jest certyfikat akredytacyjny". Generalny Inspektor proponuje posłużenie się pojęciem „udzielenia akredytacji" (konsekwentnie) albo pojęciem „certyfikat akredytacji" za rozporządzeniem 2016/679. Jednocześnie w ust. 2 pkt 3 przepisu zamiast zwrotu „okres, na jaki została udzielona akredytacja" proponuję posłużenie się zwrotem „okres ważności akredytacji".

W tym miejscu należy również podnieść, że w art. 43 rozporządzenia 2016/679 wskazano przypadki cofnięcia akredytacji. Niezasadne wydaje się więc powtarzanie tego w ust. 5 ww. przepisu projektu. Taka sama uwaga dotyczy ust. 3- czy nie jest to przeredagowanie art. 43 ust. 7 rozporządzenia 2016/679?

**9. Dokonywanie czynności sprawdzających**- w art. 9 projektu, w którym mowa jest o czynnościach sprawdzających dokonywanych po udzieleniu akredytacji, brakuje określenia szczegółowego trybu przeprowadzania tych czynności, np. elementów protokołu, postępowania po zakończeniu wskazanych czynności. Wątpliwości budzi również charakter tych czynności. W ocenie Generalnego Inspektora należy uwzględnić w projekcie przepis, z którego będzie wynikało, że do czynności sprawdzających stosuje się odpowiednio przepisy dotyczące kontroli.

**10. Pobieranie opłat**- w art. 11 projektu proponuje się wyznaczenie opłaty za udzielenie akredytacji, co oznacza, że w przypadku odmowy udzielenia akredytacji nie mogłaby być pobierana opłata za wykonane czynności. W opinii Generalnego Inspektora niewłaściwe jest uzależnianie opłaty za wykonane czynności od tego, czy akredytacja zostanie udzielona oraz niewłaściwe jest ustalenie pojedynczej stawki za cały proces i uwarunkowanie dokonania opłaty od jego wyniku (udzielenia akredytacji). Zaproponowane rozwiązanie nie byłoby spójne z innymi przepisami w tym obszarze, gdyż z art. 51 ust. 7 ustawy o systemach oceny zgodności i nadzoru rynku wynika, że za czynności związane z:

1) formalną oceną wniosku o akredytację,
2) oceną jednostki oceniającej zgodność w procesie akredytacji,
3) wystawieniem certyfikatu akredytacji,
4) sprawowaniem nadzoru nad akredytowanymi jednostkami oceniającymi zgodność,

5) uczestnictwem w krajowym systemie akredytacji

– pobiera się opłaty.

Należy mieć na uwadze, że w ww. ustawie jest przepis upoważniający ministra właściwego do spraw rozwoju w porozumieniu z ministrem właściwym do spraw finansów publicznych do określenia, w drodze rozporządzenia, sposobu ustalania opłat za czynności związane z akredytacją jednostek oceniających zgodność oraz maksymalne wysokości opłat z uwzględnieniem okoliczności, że stawki tych opłat powinny zapewnić pokrycie kosztów ich przeprowadzenia. W tym miejscu należy zasygnalizować konieczność właściwego ustalenia takiej opłaty, kryteria jej określenia oraz zasady ponoszenia. Ponadto, czy świadomą intencją prawodawcy było to aby ewentualne zmiany wysokości tej opłaty (np. waloryzacja) wiązały się z nowelizacją ustawy i uruchamianiem całego procesu legislacyjnego?

Jednocześnie w projekcie nie wskazano trybu dochodzenia zaległych, niezapłaconych opłat, terminu do ich zapłaty oraz czy nieuiszczenie opłaty będzie miało wpływ na jego ważność, czy wydanie.

W projekcie nie określono również, czyj dochód stanowią opłaty z tytułu akredytacji. Kolejna uwaga dotyczy konieczności wskazania, na jaki czas będzie wydawany certyfikat akredytacji. Ponadto w projekcie nie wskazano, czy przedłużenie (odnowienie) certyfikatu będzie podlegać opłacie.

**11. Podmioty udzielające certyfikacji (art. 12)**- W opinii Generalnego Inspektora krytycznie należy odnieść się przyjęcia rozwiązania nieprzewidującego możliwości dokonania certyfikacji przez krajowy organ nadzorczy. Możliwość taka została przewidziana w art. 42 ust. 5 rozporządzenia 2016/679. Regulując tę kwestię należy wziąć pod uwagę sytuacje, w których certyfikacja określonego obszaru będzie ekonomicznie nieopłacalna dla podmiotu certyfikującego lub też przez dłuższy czas od momentu stosowania przepisów rozporządzenia 2016/679 nie zostaną akredytowane podmioty certyfikujące. W takich sytuacjach uzasadnione wydaje się udzielanie certyfikacji przez organ nadzorczy.

Jednocześnie uwagi do opisanego w projekcie procesu certyfikacji należy odnieść analogicznie do uwag zgłoszonych do procesu akredytacji.

**12. Prowadzenie publicznie dostępnego wykazu administratorów i podmiotów przetwarzających, którym udzielono certyfikacji** - art. 14 ust. 4 projektu ustawy zobowiązuje podmiot certyfikujący do prowadzenia publicznie dostępnego wykazu administratorów i podmiotów przetwarzających, którym udzielono certyfikacji. Generalny Inspektor proponuje rozszerzyć zaproponowany obowiązek prowadzenia wykazu o obowiązek poinformowania organu nadzorczego przez podmiot certyfikujący o przyznaniu certyfikacji. Proponowana zmiana ma na celu zapewnienie, aby organ nadzorczy posiadał na bieżąco informację o administratorach i podmiotach przetwarzających, którym udzielono certyfikacji. Jest to istotne np. z punktu widzenia przeprowadzanych kontroli, ponieważ informacja o przyznanej certyfikacji umożliwi odpowiednie przygotowanie się do kontroli takich podmiotów.

**13. Uprawnienie do przeprowadzania czynności sprawdzających**- rozważając zaproponowane brzmienie art. 15 przekazanego projektu, należy zrezygnować z ust. 2. Natomiast z ust. 1 powinno

wynikać, że po udzieleniu certyfikatu, w celu oceny spełniania przez podmiot kryteriów certyfikacji podmiot certyfikujący powinien być uprawniony do podejmowania tylko takich czynności jakie podejmuje przy wydawaniu certyfikatu.

**14. Pobieranie opłaty za udzielenie certyfikacji**- w projektowanym art. 17 podano maksymalną opłatę za udzielenie certyfikacji. Ponadto w opinii Generalnego Inspektora ustawowe ograniczenie górnego poziomu opłat za udzielenie certyfikacji może zostać odebrane jako zamach na swobodę działalności gospodarczej oraz ograniczenie konkurencyjności. To administrator lub podmiot przetwarzający, w ramach posiadanego budżetu, podejmuje działania o wyborze podmiotu certyfikującego na rynku. Należy mieć na względzie, że cena jest tylko jednym z kryteriów takiego wyboru.

**15. Prezes Urzędu Ochrony Danych Osobowych**- Na wstępie uwag dotyczących kształtu organu nadzorczego Generalny Inspektor chciałby podkreślić, że przepisy rozporządzenia 2016/679 nie wymagają zmian ustrojowych w kształcie zaproponowanym przez Ministra Cyfryzacji. Obecny model funkcjonowania GIODO pod względem statusu i gwarancji niezależności zapewnia bardzo wysokie standardy i spełnia wymogi stawiane organom nadzorczym przepisami rozporządzenia. Konieczność ich wdrożenia nie powinna tych standardów obniżać. Taki pogląd znalazł również potwierdzenie w bardzo wyraźnej linii orzeczniczej Trybunału Sprawiedliwości oraz został wyrażony w doktrynie. (więcej: artykuł autorstwa Krzysztofa Rokity Europejskim Przeglądzie Sądowym 7/2016).

Odnosząc się do nazwy organu nadzorczego podkreślenia wymaga, że nie jest to kwestia kluczowa dla procesu wdrożenia przepisów rozporządzenia 2016/679. Przedstawione przez Ministra Cyfryzacji uzasadnienie dla takiej zmiany nie wydaje się jednak przekonujące. W czasie prac nad polskim tekstem ogólnego rozporządzenia ustawodawca europejski świadomie nawiązał do rozwiązań funkcjonujących od kilkunastu już lat w prawie UE. Otóż zgodnie z rozporządzeniem nr 45/2001, organem nadzorczym w zakresie przetwarzania danych osobowe przez organy i instytucje unijne jest Europejski Inspektor Ochrony Danych, a w poszczególnych organach lub instytucjach powołuje się inspektorów ochrony danych (ang. data protection officers). Również w polskim prawie można podać przykład Głównego Inspektora Pracy, inspektorów pracy czy wreszcie społecznych inspektorów pracy. Podobne w gruncie rzeczy nazwy jak dotąd nie powodowały żadnych konfuzji.

Warto też zadać sobie pytanie o koszty takiej zmiany – finansowe, prawne, ale również społeczne, dotyczące rozpoznawalności GIODO w świadomości obywateli, przedsiębiorców i administracji publicznej. Decyzja o zmianie nazwy organu powinna być więc elementem szerszej dyskusji i uwzględniać powyższe wątpliwości. Czy należy ponosić takie koszty, w sytuacji kiedy taka zmiana nie wydaje się konieczna?

Odnosząc się do przepisów rozdziału 4 projektowanej ustawy należy wskazać, że przedstawiony akt nie odnosi się do zadań organu (nawet poprzez odwołanie do przepisów rozporządzenia 2016/679).

**16. Kwalifikacje wymagane od kandydata na Prezesa Urzędu Ochrony Danych Osobowych**- art. 18 ust. 4 zawiera listę wymagań stawianych kandydatowi na Prezesa Urzędu. Na początek należy

wskazać na konieczność usystematyzowania ich według „wagi" tych wymagań. Kolejno należy wskazać, że wątpliwości budzą niektóre warunki zaproponowane w ww. przepisie.

Generalny Inspektor w przekazanych Ministrowi Cyfryzacji materiałach wskazywał, że dotychczasowe wymogi dotyczące osoby powołanej na funkcję Generalnego Inspektora są wystarczające i powinny zostać zachowane.

Jednocześnie niezrozumiałe jest zrezygnowanie (w stosunku do obecnie obowiązujących przepisów) z wymogu wyróżniania się przez kandydata na Prezesa Urzędu wysokim autorytetem moralnym. Ustawa o ochronie danych osobowych wprowadzając wymóg dotyczący charakteru osoby pełniącej funkcję Generalnego Inspektora niewątpliwie wskazuje na kryterium ocenne. Biorąc to pod uwagę podmiot zgłaszający kandydata na Generalnego Inspektora Ochrony Danych Osobowych ma obowiązek szczegółowego i przekonującego uzasadnienia, że proponowany przez niego kandydat wyróżnia się wysokim autorytetem moralnym. Niejednokrotnie zostało to już podkreślone w stanowiskach GIODO, że osoba obejmująca tę funkcję będzie odpowiadała za monitorowanie stosowania rozporządzenia w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych.

Wątpliwości natomiast budzi dopuszczalność posiadania przez kandydata wykształcenia ekonomicznego lub technicznego oraz warunek posiadania co najmniej pięcioletniego doświadczenia zawodowego w obszarze związanym z ochroną danych osobowych. Zrozumiałym wymogiem jest cecha polegająca na wyróżnianiu się doświadczeniem zawodowym. Jednakże kwestia narzucenia konkretnego okresu doświadczenia wydaje się być zbędna, zarówno w przypadku Prezesa Urzędu jak i jego zastępców. Funkcjonujący w krajowym porządku prawnym wymóg posiadania „odpowiedniego doświadczenia zawodowego" w zakresie ochrony danych osobowych związany jest z tym, że zapewnienie skuteczności nadzoru przestrzegania przepisów o ochronie danych osobowych osób fizycznych wymaga szerokiej wiedzy prawnej. Ocena, czy dany kandydat na stanowisko Generalnego Inspektora Ochrony Danych Osobowych dysponuje odpowiednim doświadczeniem, należy do posłów i senatorów decydujących o wyborze konkretnego kandydata. Rozwiązania przewidujące wybór, na podstawie kryterium wiedzy i kompetencji kandydata, m. in. Rzecznika Praw Obywatelskich, Rzecznika Praw Dziecka, kierowników centralnych urzędów administracji rządowej, prezesów agencji państwowych, nie wskazują na konkretny okres wymaganego doświadczenia zawodowego.

Odnosząc się do dopuszczalności powołania na Prezesa Urzędu Ochrony Danych Osobowych osoby posiadającej wyższe wykształcenie ekonomiczne lub technicznego należy wskazać, że istota zadań wypełnianych przez organ ochrony danych skłania do pozostawienia dotychczasowego wymogu posiadania wykształcenia wyższego prawniczego. Realizacja obowiązków w zakresie ochrony praw i wolności osób fizycznych od lat opiera się na ugruntowanym europejskim i krajowym dorobku prawnym. Zmieniające się zagrożenia technologiczne dla ochrony prywatności są tylko zjawiskami, dla których zawsze punktem odniesienia będą przyjęte normy prawne i ugruntowane orzecznictwo. Powyższe predestynuje kandydatów z wykształceniem prawniczym do pełnienia funkcji organu ochrony danych.

Zasadne wydaje się wydłużenie kadencji Prezesa Urzędu z 4 lat do 5, za przykładem takich organów jak Rzecznik Praw Dziecka, Rzecznik Praw Obywatelskich, Rzecznik Praw Pacjenta.

W art. 18 ust. 7 projektu wskazano przypadki, w których następuje wygaśnięcie kadencji Prezesa Urzędu: śmierć, odwołanie lub utrata obywatelstwa polskiego. Należy zauważyć, że dalsza

część projektu ustawy nie odnosi się do przypadku odwołania Prezesa Urzędu. Brak jest jakiejkolwiek regulacji dotyczącej przesłanek i postępowania w sprawie odwołania Prezesa Urzędu z jego funkcji. Odnosząc się natomiast do przesłanki utraty obywatelstwa polskiego należy wskazać, że utrata obywatelstwa w trakcie pełnienia funkcji Prezesa Urzędu jest równoznaczna z utratą prawa do pełnienia funkcji w tym organie.

Niedopuszczalny z punktu widzenia zagwarantowania niezależności organu ochrony danych osobowych jest również przepis art. 19 ust.3, który dotyczy możliwości wskazania przez ministra właściwego do spraw informatyzacji zastępcy Prezesa Urzędu, który pełniłby obowiązki Prezesa Urzędu, w przypadku jego odwołania. Podkreślenia wymaga, ze nawet potencjalny polityczny wpływ innych organów może skutkować zaistnieniem po stronie organu ochrony danych „przewidywanego posłuszeństwa" (ang. prior compliance). Taki pogląd znajduje szerokie uzasadnienie w bogatej linii orzeczniczej Trybunału Sprawiedliwości Unii Europejskiej. Na poziomie ustawowym powinno się uregulować zakres działania zastępców Prezesa Urzędu, a nie indywidualny akt ministra właściwego do spraw informatyzacji, który nie posiada żadnych uprawnień władczych względem organu ochrony danych osobowych.

**17. Utworzenie w Urzędzie komórki organizacyjnej do spraw rozpatrywania skarg na działalność Urzędu (art. 22 ust. 2 pkt 1)**- W ocenie Generalnego Inspektora kwestia ustanowienia komórki organizacyjnej właściwej do rozpatrywania skarg na działalność Urzędu, składanych na podstawie art. 227 Kodeksu postępowania administracyjnego, nie wymaga unormowania na gruncie regulacji ustawowej. Przedmiot wewnętrznej organizacji Urzędu powinien zostać uregulowany w akcie prawa wewnętrznego.

**18. Tajemnica (art. 23)**- Art. 54 ust. 2 rozporządzenia 2016/679 stanowi, że członek lub członkowie oraz personel każdego z organów nadzorczych podlegają zgodnie z prawem Unii lub prawem państwa członkowskiego obowiązkowi zachowania tajemnicy służbowej – w trakcie kadencji oraz po jej zakończeniu – w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wypełniania zadań lub wykonywania swoich uprawnień. Obowiązek zachowania tajemnicy służbowej w trakcie ich kadencji dotyczy w szczególności sytuacji, w których osoby fizyczne zgłaszają naruszenia niniejszego rozporządzenia. W ocenie Generalnego Inspektora ww. zasada nie wymaga „przepisania" do nowej ustawy o ochronie danych osobowych i nie wymaga również jej rozszerzenia na wszelkie „informacje, o których (Prezes urzędu, zastępcy Prezesa Urzędu oraz pracownicy Urzędu) dowiedzieli się w związku z wykonywaniem czynności służbowych".

**19. Rada do Spraw Ochrony Danych Osobowych (art. 24)**- przekazany projekt ustawy nie zawiera uzasadnienia, stąd trudno jest ocenić zasadność powołania przy Prezesie Urzędu Rady do Spraw Ochrony Danych Osobowych. Z zaproponowanego brzmienia art. 24 nie wynika, czy powołana Rada ma mieć charakter niezależny, skąd wynika wskazany zakres podmiotów, które mogą rekomendować członków Rady oraz dlaczego zakres działania Rady pokrywa się z zadaniami nałożonymi na Prezesa Urzędu Ochrony Danych Osobowych. Przedstawiony w projekcie zakres zadań Rady podważa kompetencje Prezesa Urzędu i jednocześnie przeczy założeniom określonym w ust. 1 , że jest ona „organem opiniodawczo- doradczym" Prezesa Urzędu.

Funkcjonowanie ciała doradczego przy Generalnym Inspektorze nie jest rozwiązaniem nowym, przez wiele lat przy GIODO funkcjonowała Rada Naukowa. Obecnie Generalny Inspektor wspierany jest wiedzą i doświadczeniem wybitnych polskich naukowców skupionych w Komisji Ekspertów GIODO. Sposób i tryb działania tych ciał był każdorazowo określany przez organ ochrony danych przy poszanowaniu zasady, że Generalny Inspektor nie jest związany żadnymi opiniami i wytycznymi przygotowanymi przez te zespoły.

Wątpliwości budzi również kwestia powoływania członków Rady oraz upoważnienie do wydania przez ministra właściwego do spraw informatyzacji rozporządzenia określającego wysokość wynagrodzenia członka Rady. Biorąc pod uwagę fakt, że wynagrodzenie będzie ustalał minister właściwy do spraw informatyzacji powstaje pytanie, jak wpłynie to na kształtowanie budżetu Prezesa Urzędu Ochrony Danych Osobowych i jego niezależność w aspekcie rozporządzania tym budżetem. Jest to kolejny przykład niedopuszczalnej sytuacji, kiedy minister właściwy do spraw informatyzacji będzie miał istotny wpływ na funkcjonowanie niezależnego organu ochrony danych.

Pojawiają się również nieścisłości w kontekście członków powoływanych w skład Rady- obecne brzmienie art. 24 ust. 9 projektu wskazuje, że kandydaci rekomendowani przez Prezesa Urzędu Komunikacji Elektronicznej oraz Prezesa Urzędu Ochrony Konkurencji i Konsumentów nie będą mogli wejść w skład Rady do Spraw Ochrony Danych Osobowych.

**20. Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych (art. 25)**- Zgodnie z art. 59 rozporządzenia 2016/679 roczne sprawozdanie z działalności organu nadzoru są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem państwa członkowskiego. Zaproponowany przepis projektu ustawy budzi wątpliwości co do swojej zasadności. W szczególności nie wynika z niego, czy jest to sprawozdanie, o którym mowa w art. 59 rozporządzenia 2016/679 czy jest to inny rodzaj sprawozdania. Niezrozumiała jest kwestia nieprzedstawienia przez Ministra Cyfryzacji podmiotów, którym Prezes Urzędu przedstawia sprawozdanie, skoro większość z nich wynika ze wskazanego przepisu rozporządzenia. Generalny Inspektor sugeruje przedstawienie sprawozdania, o którym mowa w art. 59 rozporządzenia 2016/679 również Rzecznikowi Praw Obywatelskich.

Jednocześnie należy zauważyć, że w przedstawionym projekcie w art. 25 brakuje ust. 2 i 3. Natomiast w ust. 4 omawianego przepisu jest mowa o „opinii". Z przepisów nie wynika jednak o jaką opinię chodzi, dlatego trudno jest odnieść się do tej propozycji brzmienia tego przepisu. Powstaje tu również pytanie o to, jaki charakter będzie miała ta opinia i jakie konsekwencje będzie wywoływała ewentualna negatywna opinia.

**20. Wymóg konsultowania projektów aktów prawnych dotyczących ochrony danych osobowych (art. 26)** – Proponuję przeredagowanie przepisu w następujący sposób: „Projekty ustaw, umów międzynarodowych i rozporządzeń dotyczące ochrony danych osobowych podlegają uzgodnieniom z Prezesem Urzędu."

**21. Monitorowanie przestrzegania kodeksów postepowań ( art. 29- 31)**- W przepisach art. 29- 31 znajdują się regulacje dotyczące obowiązku nałożonego na podmiot akredytowany (art. 29) oraz uzyskania akredytacji (art. 30) i wymagań dotyczących certyfikatu akredytacyjnego(art. 31). W opinii Generalnego Inspektora ww. przepisy nie powinny się znaleźć w rozdziale dotyczącym

organu nadzorczego. Jednocześnie, w tym miejscu należy zauważyć, że w projekcie nie ma regulacji odnoszącej się do konsultacji i zatwierdzania kodeksu postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, a zaproponowane brzmienie art. 29 projektu jest powtórzeniem treści art. 41 ust. 1 rozporządzenia 2016/679.

**22. Wykaz rodzajów operacji przetwarzania danych osobowych, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679 (art. 32)**- Minister Cyfryzacji zaproponował w art. 32 ust. 2 projektowanej ustawy aby wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych był podawany do publicznej wiadomości poprzez ogłoszenie w Dzienniku Urzędowym RP „Monitor Polski". Należy przeanalizować, czy zaproponowany zapis nie jest nadmiarowy i czy nie wystarczyłoby opublikowane tej informacji w Biuletynie Informacji Publicznej Urzędu, gdzie zamieszczane będą również standardowe klauzule umowne, zatwierdzone kodeksy postępowania oraz inne ważne, z punktu widzenia obywatela i przedsiębiorcy informacje i dokumenty.

**23. Procedura uprzednich konsultacji (art. 33)** - Projektowany art. 33 ogranicza możliwość zawieszenia biegu terminów do jednego razu i na okres nie przekraczający 14 dni. Zgodnie z art. 36 ust. 2 rozporządzenia 2016/679, bieg terminów na udzielenie pisemnego zalecenia można zawiesić do czasu, aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji. Powstaje zatem wątpliwość, czy dopuszczalne jest takie „doprecyzowanie" art. 36 ust. 2 rozporządzenia 2016/679 na podstawie przepisów krajowych.

**24. Dokonywanie zgłoszenia naruszenia ochrony danych (art. 34)**- W ocenie Generalnego Inspektora zaproponowane brzmienie art. 34 jest niewystarczające. Na dalszym etapie prac legislacyjnych Generalny Inspektor przedstawi niezbędne uzupełnia w tym zakresie.

**25. Jednoinstancyjność postępowania (art. 37 ust. 2)** - Generalny Inspektor z zadowoleniem przyjmuje, iż propozycja, przekazana w wytycznych GIODO oraz projekcie przepisów przekazanych Ministrowi Cyfryzacji, by postępowanie prowadzone przed krajowym organem nadzorczym było jednoinstancyjne została przyjęta przez Ministra. Jednak wiele elementów z zaproponowanej przez Generalnego Inspektora procedury postępowania przed organem nie zostało uwzględnione. W ocenie Generalnego Inspektora przyjęty przez nas model zapewniał skuteczniejszą realizację zadań krajowego organu ochrony danych.

**25. Udział organizacji społecznej w postępowaniu**- w art. 38 projektu zaproponowano ograniczenie uprawnienia organizacji społecznych do występowania w sprawach z zakresu ochrony danych osobowych w porównaniu z propozycją procedury GIODO (art. 7 przedstawionej przez GIODO propozycji) oraz obowiązującym art. 31 – Kodeksu postępowania administracyjnego, które mogły być szerszym urzeczywistnieniem konstrukcji przewidzianej w art. 80 ust. 2 rozporządzenia 2016/679. Projekt Ministra Cyfryzacji przewiduje, że organizacja, aby mogła żądać wszczęcia lub dopuszczenia do udziału w postępowaniu, będzie musiała:

1) wykazać naruszenie praw podmiotu danych oraz
2) wskazać, że za uwzględnieniem ich żądania wszczęcia lub dopuszczenia do udziału w postępowaniu przemawia interes osoby, której prawa zostały naruszone.

Zaproponowany przepis projektu ustawy rodzi po stronie organu ochrony danych konieczność przeprowadzenia postępowania co do zaistnienia ww. przesłanek. Jednocześnie zauważyć należy, że – zgodnie z art. 53 projektu ustawy – rozstrzygnięcie organu nadzorczego w przedmiocie dopuszczenia organizacji społecznej do występowania w sprawach z zakresu ochrony danych osobowych jest niezaskarżalne. Biorąc pod uwagę postanowienia art. 80 rozporządzenia 2016/679 wypadałoby rozważyć prawidłowość rozwiązania zaproponowanego w art. 38 projektu ustawy.

**26. Niezałatwienie sprawy w terminie** - przedstawiona w art. 39 projektu ustawy propozycja idzie dalej niż zaproponowane przez GIODO przepisy oraz planowany kształt ustawy- Kodeks postępowania administracyjnego. Art. 9 zaproponowanej procedury GIODO przewidywał szczególną wobec art. 37 Kodeksu postępowania administracyjnego regulację instytucji ponaglenia, które nie zwiększałoby obciążeń administracyjnych organu, a jednocześnie umożliwiało stronie wpłynięcie na przyśpieszenie czynności dokonywanych przez organ. Celem tej propozycji było unikanie prowadzenia przez organ postępowań incydentalnych, aby jak najszybciej zakończyć postępowanie i zapewnić przestrzeganie przepisów o ochronie danych osobowych. Natomiast Minister Cyfryzacji zaproponował wyłączenie obowiązku organu pozostającego w zwłoce do pouczenia strony o możliwości złożenia ponaglenia. Jednocześnie przepisy art. 37 Kodeksu postępowania administracyjnego nadal umożliwiają stronie wniesienie takiego ponaglenia, które zainicjuje czasochłonne postępowanie zmierzające do wyjaśnienia przyczyn przewlekłości lub bezczynności.

**27. Przedstawienie przez stronę dowodu**- w art. 40 projektu Minister Cyfryzacji posłużył się w całości rozwiązaniem z art. 189 ustawy z dnia 29 sierpnia 1997r.- Ordynacja podatkowa (Dz. U. z 2017 r. poz. 201, z późn. zm.). Jednocześnie w projektowanych przepisach nie wskazano sankcji za nieprzedstawienie dowodu. Dodatkowo należy stwierdzić, iż zakreślenie minimalnego terminu może prowadzić do przedłużenia postępowania, zwłaszcza gdy strona złoży wniosek o przedłużenie terminu do przedstawienia dowodu. Może to negatywnie wpłynąć na wypełnienie obowiązku organu do zakończenia postępowania w terminie 1 miesiąca. Zaczerpnięcie rozwiązania z przepisów regulujących postępowanie przed organami podatkowymi, w którym co do zasady występuje tylko jedna strona, nie odpowiada realiom postępowań prowadzonych przed organem ochrony danych osobowych, w których występuje podmiot danych, jako osoba poszkodowana przez działanie albo jego brak po stronie administratora danych.

Rozważenia wymaga, czy krajowy organ nadzoru będzie przyjmował każde tłumaczenie od strony dokumentacji sporządzonej w języku obcym, czy tylko poświadczone przez tłumacza przysięgłego (art. 40 ust. 3 projektu).

**28. Prawo dostępu do informacji**- propozycja ujęta w art. 41 projektu ustawy stanowi powtórzenie przepisów dotyczących tajemnic ustawowo chronionych i wydaje się zbędna z punktu widzenia zasad racjonalnej legislacji. Odczytując dosłownie brzmienie tego przepisu- ust. 1 ogranicza uprawnienia organu ochrony danych ze względu na przepisy odrębnych ustaw, zaś ust. 2 umożliwia działanie organowi ochrony danych, jeżeli te ustawy tak stanowią. Konsekwencją takiego brzmienia art. 40 projektu będzie brak dostępu organu do tajemnic ustawowo chronionych, w sytuacji gdy przepisy szczególne regulujące dostęp do tych tajemnic, nie będą

uwzględniały ww. organu jako uprawnionego do dostępu. Co za tym idzie, takie rozwiązanie w praktyce oznaczać będzie ograniczenie lub nawet uniemożliwienie realizacji jego zadań.

Wprowadzone ograniczenie dostępu organu do informacji, które strona może uznać za informacje ustawowo chronione, pozostaje w sprzeczności chociażby z art. 42 ust. 6 rozporządzenia 2016/679, który nie ogranicza dostępu do informacji, niezbędnych do przeprowadzenia certyfikacji nawet w odniesieniu do podmiotu certyfikującego. Ograniczenie takie tym bardziej nie powinno odnosić się do organu nadzorczego. Patrząc na zakres uprawnień już dziś przysługujących GIODO na podstawie ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Systemie Informacji Wizowej (Dz. U. z 2014 r. poz. 1203) i ustawy z dnia 16 września 2011 r. o wymianie informacji pomiędzy organami ścigania państw członkowskich Unii Europejskiej (Dz. U. z 2011 r. Nr 203, poz. 1371), które gwarantują dostęp celem skutecznego prowadzenia postępowań, projektodawca powinien wskazać *ratio legis* tej propozycji.

**29. Zastrzeżenie informacji stanowiących tajemnicę przedsiębiorstwa-** w art. 42 ust. 2 projektowanej ustawy zaproponowano przepis: „Prezes Urzędu może uchylić zastrzeżenie w drodze decyzji, jeżeli uzna, że informacje, dokumenty lub ich części nie spełniają przesłanek do objęcia ich tajemnicą przedsiębiorstwa". Przepis ten w zaproponowanym kształcie wydaje się niewykonalny z uwagi na to, że wymaga on od organu nadzoru oceny, czy wskazane przez stronę ograniczenie dostępu do informacji i dokumentów spełnia przesłanki do objęcia ich tajemnicą przedsiębiorstwa. W opinii Generalnego Inspektora nie jest to możliwe bez zapoznania się z treścią takich dokumentów.

Jednocześnie przewidziana w art. 42 ust. 2 projektu forma decyzji, którą organ będzie mógł uchylić zastrzeżenie tajemnicy przedsiębiorstwa, wydłuży postępowanie przed organem z uwagi na konieczność przeprowadzenia postępowania incydentalnego.

W związku z natychmiastową wykonalnością decyzji organu ochrony danych (zgodnie z art. 52 projektu ustawy) informacje objęte tajemnicą przedsiębiorstwa zostaną, natychmiast po wydaniu przez organ ochrony danych decyzji o uchyleniu zastrzeżenia tajemnicy przedsiębiorstwa, ujawnione w aktach sprawy, zanim strona niezadowolona z takiej decyzji organu ochrony danych będzie mogła złożyć skargę do sądu administracyjnego. W przypadku przychylenia się sądu administracyjnego do skargi, po stronie skarżącego powstanie uprawnienie do dochodzenia odszkodowania od Skarbu Państwa z powodu bezprawnego ujawnienia tajemnicy jego przedsiębiorstwa. W opisywanej sytuacji bowiem tajemnica przedsiębiorstwa została już ujawniona w aktach postępowania, z którymi mogą zapoznać się pozostali uczestnicy postępowania.

**30. Ograniczenie prawa do wglądu do materiału dowodowego-** W art. 43 projektu ustawy przyjęto, inaczej niż w propozycji przepisów GIODO, że postanowienie o ograniczeniu prawa do wglądu do materiału dowodowego byłoby zaskarżalne tylko wraz z decyzją kończącą postępowanie (zgodnie z art. 53 projektu). Przepisy zaproponowane przez GIODO zakładały, że do kontroli takiego postanowienia może dojść już po jego wydaniu, co stanowiłoby gwarancję ochrony tajemnicy przedsiębiorstwa. Propozycja Ministra Cyfryzacji nie zachowuje równowagi pomiędzy prawami podmiotów danych a przedsiębiorców, co miało być głównym celem działania

Ministra Cyfryzacji. Istnieje obawa, że może dochodzić do celowego przedłużania postępowania przed organem ochrony danych, a tym samym ograniczenia realizacji praw podmiotów danych zagwarantowanych w rozporządzeniu 2016/679.

Proponowane brzmienie art. 43 ust. 5 może spowodować, że przedsiębiorcy będą informować organ, iż całość informacji zawieranej w dokumentach stanowi tajemnicę przedsiębiorstwa, nie dokonując szczegółowej analizy jego treści, która to analiza powinna być dokonana przez przedsiębiorcę przed złożeniem wniosku o wyłączenie informacji stanowiących tajemnicę przedsiębiorstwa. Konsekwencją proponowanej regulacji będzie to, że w przypadku gdy jedynie niektóre informacje zawarte w dokumencie stanowić będą tajemnicę przedsiębiorstwa, organ będzie zmuszony ograniczyć dostęp do materiału dowodowego pozostałym stronom prowadzonego postępowania w zakresie całego dokumentu. Tym samym strony postępowania, nie będą mogły zapoznać się z pozostałymi, niestanowiącymi tajemnicy przedsiębiorstwa, informacjami zawartymi w tym dokumencie. Wskazać należy, iż polski ustawodawca, w przypadku ograniczenia dostępu do materiału dowodowego z uwagi na tajemnicę przedsiębiorstwa, przewiduje możliwość wyłączenia określonej informacji, nie zaś całego dokumentu [tak również: art. 69 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. 2017 r. poz. 299)]. Ponadto podkreślić trzeba, iż wyłączeniu podlegać może jedynie treść dokumentu stanowiąca tajemnicę przedsiębiorstwa, nie zaś jego forma, która może mieć istotne znaczenie dla strony w toku prowadzonego postępowania (w tym m. in. cechy fizyczne dokumentu, rodzaj lub wzór podpisu). W ocenie Generalnego Inspektora, utrzymanie obowiązku przedstawienia dokumentu niezawierającego tajemnicy przedsiębiorstwa, zgodnie z art. 43 ust. 2 projektu, powoduje, iż przedsiębiorcy będą zmuszeni wykazywać należytą staranność, szczegółowo uzasadniając wyłączenie poszczególnych informacji zawartych w przedkładanych dokumentach.

**31. Kara grzywny**- w art. 44 projektu ustawy przewiduje się karę grzywny do 500 zł dla osoby, która będąc obowiązana do osobistego stawienia się jako świadek lub biegły, mimo prawidłowego wezwania, nie stawiła się bez uzasadnionej przyczyny albo bezzasadnie odmówiła złożenia zeznania, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej. Minister Cyfryzacji we wprowadzeniu do projektu ustawy nie wskazał, czym kierował się ustalając karę grzywny w takiej wysokości.

Należy również wziąć pod uwagę, że kara może obejmować zarówno świadka, który nie stawia się na wezwanie organu, jak i osobę, która w toku kontroli prowadzonej przez organ odmawia złożenia zeznania bądź okazania przedmiotu oględzin. Proponowaną karę w wysokości 500 zł można ewentualnie przewidzieć za unikanie zeznań świadka lub biegłego, a nie wobec osoby reprezentującej podmiot, w którym prowadzone są czynności kontrolne na miejscu, czy wobec którego prowadzone jest postępowanie. Niektóre przepisy w polskim prawie przewidują znacznie większe kary za unikanie obowiązków związanych ze składaniem wyjaśnień czy wydawaniem opinii. W ustawie z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2017r. poz.229) art. 114 przewiduję karę grzywny nie mniejszą niż 2000 zł dla przedsiębiorcy, który wbrew obowiązkowi, nie udziela rzecznikowi konsumentów wyjaśnień i informacji będących przedmiotem wystąpienia oraz nie ustosunkowuje się do uwag i opinii rzecznika. Innym przykładem może być art. 56b ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2016 r. poz. 2046). We

wspomnianym przepisie przewidziana jest kara grzywny do 5000 zł dla osób, które zgłaszają nieprawdziwe dane lub udzielają nieprawdziwych wyjaśnień lub odmawiają ich udzielenia.

Minister Cyfryzacji zaproponował 5-krotne obniżenie wysokości kary grzywny za bezzasadną odmowę złożenia zeznania w porównaniu z art. 17 propozycji przepisów przygotowanych przez GIODO. Można stwierdzić, iż nie jest to kwota wysoka w stosunkach społeczno-gospodarczych, a zatem nie ma charakteru przymuszającego do wypełnienia obowiązku nakładanego przez organ i może prowadzić do utrudniania prowadzenia postępowania.

**32. „Odrębne" postępowanie kontrolne**- w art. 45 projektu mowa jest o możliwości prowadzenia postępowania kontrolnego (odrębnie uregulowanego) w toku postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. Wydaje się jednak, że – tak jak to się odbywało dotychczas – postępowanie kontrolne powinno być prowadzone w związku z innym postępowaniem, niejako na jego potrzeby, a nie w jego ramach. Przy pozostawieniu takiego uregulowania pojawiają się takie wątpliwości, jak np. kwestia statusu materiału dowodowego, tzn. czy akta kontroli miałyby stanowić część akt innego postępowania, a więc, czy strona tego postępowania (np. osoba składająca skargę) miałaby prawo przeglądania również akt kontroli. W tym miejscu należy podtrzymać brzmienie art. 16 propozycji GIODO dotyczącej prowadzenia czynności kontrolnych w postępowaniu. W ww. przepisie propozycji GIODO potwierdzono, znajdującą już oparcie w orzecznictwie, koncepcję, iż czynności kontrolne mają charakter odrębny od postępowania administracyjnego. Dlatego istnieje potrzeba jednoznacznego wskazania, że takie odrębne czynności kontrolne mogą stać się częścią postępowania administracyjnego i stanowić dowody w postepowaniach prowadzonych na podstawie rozporządzenia 2016/679. Nadmienić należy, iż możliwość takiego pozyskania dowodów istnieje już w aktualnym stanie prawnym. Brzmienie przepisu zaproponowanego przez GIODO pozwala uniknąć wątpliwości terminologicznej sprowadzającej się do „prowadzenia postępowania w postępowaniu", tj. prowadzenia odrębnego postępowania kontrolnego w postępowaniu administracyjnym.

**33. Ograniczenie przetwarzania danych**- Wątpliwości budzi relacja art. 46 ust. 1 projektu ustawy do art. 58 ust.2 lit. f rozporządzenia 2016/679 dotyczącego uprawnienia naprawczego organu nadzorczego. Komentowany przepis projektu Ministra Cyfryzacji wprowadza, nieprzewidziane w rozporządzeniu 2016/679, przesłanki warunkujące zastosowanie instytucji ograniczenia przetwarzania danych. Tym samym wątpliwe jest jego brzmienie, a nawet kwestia dopuszczalności jego wprowadzenia, gdyż wydaje się sprzeczny z ww. przepisem rozporządzenia 2016/679. Przypomnieć należy, że przepisy prawa krajowego nie mogą modyfikować bezwzględnie wiążących norm zawartych w rozporządzeniach unijnych. Rozporządzenia unijne, zgodnie z Traktatem o funkcjonowaniu Unii Europejskiej, stosowane są w państwach członkowskich bezpośrednio.

**34. Decyzja o umorzeniu postępowania**- w art. 47 projektu ustawy wprowadzono obligatoryjne wydawanie przez organ decyzji o umorzeniu postępowania. Przepis ten jest zbędny, gdyż bardziej prawidłowym jest dotychczas stosowane rozwiązanie prawne polegające na łączeniu spraw w przypadku ponownego (kolejnego) wniesienia przez stronę tej samej sprawy do organu. Przyjęcie zaś rozwiązania zaproponowanego w projekcie skutkować może niepotrzebnym zwiększeniem obciążeń organu (konieczność wydania decyzji administracyjnej, ewentualna potrzeba udzielania

odpowiedzi na skargę strony na tę decyzję itd.). Utrudni to zakończenie postępowania właściwego w terminach przewidzianych w Kodeksie postępowania administracyjnego.

Należy podkreślić, że jest to kolejny przykład wprowadzenia dodatkowego postępowania incydentalnego, zamiast skoncentrowania się na prowadzeniu postępowania głównego. Stosowane chętnie przez Generalnego Inspektora w aktualnym stanie prawnym łączenie spraw ułatwia i przyśpiesza postępowanie. Odejście od obecnej praktyki będzie przedłużać postępowanie, narażać organ ochrony danych na zarzuty przewlekłości i naruszać prawa osób, których dane dotyczą.

**35. Udzielenie upomnienia**- projektowany art. 49 stanowi, że w przypadku gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia, Prezes Urzędu może w drodze decyzji udzielić upomnienia. Wynikające z art. 58 ust. 2 rozporządzenia 2016/679 uprawnienia organu nadzorczego zawierają m.in. upomnienie. Projektodawca wprowadza jednak, wzorem ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 2016 r. poz. 1137), stopniowanie wagi naruszenia przepisów (znikoma społeczna szkodliwość czynu). Niedopuszczalne jest wprowadzenie w ustawie krajowej dodatkowych przesłanek zastosowania instytucji wprost przewidzianej w rozporządzeniu (upomnienia). Podnieść należy, iż rozporządzenie nie przewiduje pojęcia „znikomości" naruszenia, a tym samym pojęcie takie nie może być wprowadzone w przepisie krajowym w odniesieniu do stosowania instytucji prawnej upomnienia.

**36. Udostępnianie decyzji Prezesa Urzędu na stronach BIP (art. 50)**- W ocenie Generalnego Inspektora art. 50 projektu ustawy jest zbędny.

**37.** Wyłączenie zaproponowane w art. 51 ust. 1 projektu ustawy ograniczałoby uprawnienie organu do kontrolowania prawidłowości przetwarzania danych o poglądach politycznych, które zgodnie z art. 9 rozporządzenia 2016/679 zawierają się w pojęciu szczególnych kategorii danych osobowych. Istnieje wątpliwość, czy takie ograniczenie jest zatem zgodne z rozporządzeniem 2016/679, które tylko w motywie nr 56 odnosi się do kwestii działań związanych z wyborami. Jest to zatem konstrukcja wyłączenia nieznana przepisom rozporządzenia 2016/679 ani w zakresie przedmiotowym, ani podmiotowym. Należy wskazać, iż w ocenie Generalnego Inspektora ust. 2 komentowanego przepisu odnosi się do treści 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 (Dz. Urz. UE L 119 z 04.05.2016 r., str. 89), tzw. dyrektywy policyjnej. Powstaje zatem wątpliwość, czy to wyłączenie powinno być przedmiotem prac legislacyjnych prowadzonych przez Ministra Cyfryzacji.

**38. Rygor natychmiastowej wykonalności**- Zaproponowane brzmienie art. 52 projektu ustawy budzi zasadnicze wątpliwości. Przyjęcie, zaproponowanego w tym przepisie, rozwiązania w istocie pozbawia adresata decyzji jakichkolwiek praw procesowych. Skoro bowiem każda (z wyjątkiem sytuacji przewidzianej w ust. 2) decyzja organu jest natychmiast wykonalna, to skuteczność tej

decyzji powstaje już z chwilą jej podpisania przez organ nadzorczy. Oznacza to, że decyzja taka może być skierowana przez organ do przymusowego wykonania natychmiast po jej podpisaniu, zanim adresat tej decyzji miałby możliwość zapoznania się z jej treścią. Adresat decyzji jest zatem pozbawiony (w każdym przypadku) możliwości dobrowolnego dostosowania się do jej treści. Co więcej, odczytując literalnie art. 52 ust. 2, wstrzymanie wykonania decyzji może odnosić się jedynie do kwestii, zawartego w niej rozstrzygnięcia w przedmiocie administracyjnej kary pieniężnej. Tym samym inne, potencjalnie wcale nie mniej dolegliwe dla adresata decyzji, rozstrzygnięcia takie jak zakaz przetwarzania danych osobowych, nakaz usunięcia danych osobowych podlegałyby nieodwołalnemu, natychmiastowemu wykonaniu po podpisaniu decyzji.

W swojej propozycji Generalny Inspektor zauważył wyżej wymieniony problem i dlatego przyjął, że wydawane przez niego decyzje będą skuteczne i wykonalne dopiero od chwili ich doręczenia adresatowi. Taka, zaproponowana przez GIODO, konstrukcja przepisów po pierwsze zapewniałaby adresatom decyzji możliwość zapoznania się z nimi i dobrowolnego dostosowania się do żądań GIODO, po drugie zaś – realnie umożliwiałaby adresatom decyzji skorzystanie z przysługujących im środków procesowych, takich jak wniosek o wstrzymanie wykonalności decyzji skierowany do sądu administracyjnego.

**39. Skarga na decyzję-** Inaczej niż w propozycji GIODO, rozwiązanie przedstawione w art. 53 projektu znacznie ogranicza uprawnienia stron do zaskarżania postanowień wydanych w toku postępowań prowadzonych przez organ. Co więcej, zaproponowane brzmienie przepisu nasuwa wątpliwość, czy uprawnienie do zaskarżania postanowień jest ograniczone tylko do stron postępowania, a tym samym czy inne osoby będące adresatami postanowień, a niebędące stronami postępowania są w ogóle pozbawione uprawnienia do zaskarżania postanowień naruszających ich prawa. Z drugiej zaś strony, jeśli do tych innych osób stosowałyby się ogólne przepisy Kodeksu postępowania administracyjnego, to powstałaby dość kuriozalna sytuacja, w której uprawnienia tych osób (w zakresie zaskarżania postanowień) byłyby szersze, niż uprawnienia stron postępowania.

**40. Tryb autokontroli-** regulacja przewidziana w art. 54 projektu (odmienna niż przewidziana w art. 24 propozycji przepisów GIODO) uniemożliwia organowi przeprowadzenie dodatkowych czynności podejmowanych w celu wyjaśnienia okoliczności podnoszonych w skardze do sądu administracyjnego, a mających istotne znaczenie dla przedmiotu sprawy. Stoi to w sprzeczności z celem postępowania prowadzonego przed organem, które ukierunkowane jest na zapewnienie skutecznej i szybkiej ochrony podmiotowi danych. Uniemożliwienie organowi przeprowadzenia dodatkowych czynności wyjaśniających w ramach tzw. autokontroli, w powiązaniu ze stosunkowo krótkim terminem na wydanie nowej decyzji, rodzi pytanie o realną skuteczność tej instytucji prawnej.

**41. Wyłączenia-** W art. 55 projektowanej ustawy przewidziano wyłączenie stosowania jedynie przepisów dotyczących: zasady ugodowego załatwiania sprawy, prowadzenia metryki sprawy, ugody administracyjnej. W przekazanej przez Generalnego Inspektora propozycji przepisów przyjęto odmienną filozofię stosowania Kodeksu postępowania administracyjnego. Po kompleksowej analizie przepisów KPA Generalny Inspektor wybrał tylko te przepisy, które są

rzeczywiście przydatne dla szybkiego i skutecznego rozpatrywania spraw wniesionych przez obywateli.

Przykładowo wskazać należy choćby tak istotne niekonsekwencje przyjętych w projekcie Ministra Cyfryzacji regulacji, jak:

- wyłączenie ugody administracyjnej (z czym GIODO się zgadza) przy jednoczesnym pozostawieniu obowiązywania przepisów nowego KPA dotyczących mediacji (art. 96a–96n KPA),
- wprowadzenie w art. 37 ust. 2 projektu zasady jednoinstancyjności postępowania przed organem przy jednoczesnym zachowaniu zastosowania przepisów KPA dotyczących postępowania odwoławczego i zażaleniowego (art. 127-144 KPA) poprzez ich niewyłączenie w art. 55 projektu,
- stosowanie przepisów KPA przewidujących zażalenia na poszczególne incydentalne postanowienia organu, w sytuacji gdy postępowanie przed organem ma być jednoinstancyjne (np. art. 31 § 2 KPA, art. 59 § 1 KPA, art. 61a § 2 KPA),
- przewidywanie stosowania nieprzydatnego w istocie przepisu KPA dotyczącego sporów o właściwość (art. 22 KPA), w sytuacji gdy przepis ten nie reguluje sposobu rozstrzygnięcia sporu między organem niezależnym, jakim jest i ma być organ ochrony danych a innymi organami, w szczególności należącymi do administracji publicznej (dla porównania w propozycji GIODO zagadnienie to zostało unormowane w art. 5 przy jednoczesnym wyłączeniu stosowania art. 22 KPA).

**42. Europejska współpraca administracyjna**- W przekazanych Ministrowi Cyfryzacji wytycznych wskazano, że należy rozważyć w jakiej prawnej formie będzie działał organ nadzorczy wydając środki tymczasowe. Minister Cyfryzacji w przekazanym projekcie przyjął, że będzie to postanowienie (art. 56 projektu ustawy). Jednocześnie w wytycznych GIODO (str. 9) zwrócono uwagę na konieczność określenia zasad tłumaczenia dokumentów przedstawionych w języku obcym. Trudno uznać, że art. 57 określa zasady tłumaczenia dokumentów. Z przedmiotowego przepisu nie wynika, kto będzie mógł przetłumaczyć takie dokumenty, czy wymagane będzie tłumaczenie dokonane przez tłumacza przysięgłego.

**43. Postępowanie kontrolne**- z art. 59 ust. 1 projektu wynika, że organ nadzorczy może prowadzić kontrole przestrzegania przepisów o ochronie danych osobowych. Wydaje się, że powinno zostać wprost wskazane, iż nie tyle „może" realizować to zadanie (co sugeruje tylko możliwość, a nie konieczność), co realizuje je będąc do tego obowiązany. Należy wskazać, że nie jest to zadanie fakultatywne tylko obligatoryjne.

W art. 36 ust. 2 projektu mowa jest z kolei o prowadzeniu kontroli na podstawie zatwierdzonych przez Prezesa Urzędu planów kontroli bądź poza nimi. Niezrozumiałe jest użycie w tym przepisie słowa „również", ze względu na nie sens przepisu jest taki, iż poza kontrolami, o których mowa w art. 36 ust. 1 projektu, mogą być prowadzone jeszcze inne kontrole. Wydaje się jednak, że intencją projektodawcy było wskazanie, iż kontrole, o których mowa w ust. 1 powołanego artykułu mogą być prowadzone w dwojaki sposób: zgodnie z planem lub poza nim.

**44. Kontrolujący**- w art. 60 projektu również użyto słowa „może" w odniesieniu do prowadzenia kontroli przez upoważnionego pracownika oraz w odniesieniu do upoważniania członków lub

pracowników organu nadzorczego państwa członkowskiego Unii Europejskiej. Również w tym miejscu należy wskazać wprost, że kontrolę prowadzą upoważnieni pracownicy, a organ nadzorczy wydaje ww. upoważnienia. Ponadto brak jest w ust. 1 powołanego artykułu wskazania, kto upoważnia pracownika do przeprowadzenia kontroli.

**45. Upoważnienie do przeprowadzenia kontroli**- W projektowanych przepisach brakuje regulacji dotyczącej obowiązku okazania upoważnienia i legitymacji przez kontrolującego (mowa jest tylko o takim obowiązku w razie nieobecności kontrolowanego- art. 62 ust. 2 projektu).

W art. 62 ust. 1 pkt 4 projektu, w którym wymienia się jeden z elementów upoważnienia do przeprowadzenia kontroli, określenie „okresu objętego kontrolą" jest zbędne, gdyż stanowi to nieuzasadnione zawężenie, bowiem niejednokrotnie dopiero w toku kontroli można stwierdzić, np. kiedy doszło do konkretnego naruszenia przepisów.

Ze względu na różny stopień skomplikowania stanów faktycznych, które są przedmiotem kontroli, Generalny Inspektor widzi konieczność umożliwienia uczestnictwa w kontroli osobom posiadającym specjalną wiedzę czy umiejętności. Wskazać należy, że taką możliwość przewiduje choćby art. 13 ust. 3 ustawy z dnia 15 grudnia 2000 r. o Inspekcji Handlowej (Dz. U. z 2017 r. poz. 1063). Wydaje się zatem, iż podobne rozwiązanie prawne mogłoby być wprowadzone do ustawy o ochronie danych osobowych.

**46. Uprawnienia kontrolującego**- Art. 63 projektu stanowi, że „w celu uzyskania informacji mogących stanowić dowód w sprawie (...) kontrolujący ma prawo wykonywania czynności kontrolnych określonych katalogu zawartym w ust.1 tego artykułu. Takie określenie celu kontroli jest zbyt wąskie. Kontrola - co do zasady - polega na badaniu stanu faktycznego w celu porównania go z obowiązującym prawem i zastosowaniu odpowiednich środków jeśli stan faktyczny jest niezgodny z prawem. Zawężanie celu do „uzyskania dowodów w sprawie" może zaistnieć w sytuacji określonej w projektowanym art. 23, dotyczącym kontroli w toku postępowania (np. skargowego). Projektodawca w ww. przepisie wskazał, iż kontrolujący ma prawo do wstępu na grunt oraz do budynków (...), wglądu do wszelkich dokumentów (...), przeprowadzenia oględzin (...), czy też żądania złożenia pisemnych lub ustnych wyjaśnień (...). Jest to katalog zamknięty, bowiem w powyższym artykule nie użyto zwrotu „w szczególności". Ponadto takie sformułowanie przepisu nie formułuje jasno, iż kontrola może być przeprowadzona w obecności kontrolowanego lub osoby przez niego upoważnionej w siedzibie kontrolowanego lub w miejscu wykonywania działalności oraz w godzinach pracy lub w czasie faktycznego wykonywania działalności przez kontrolowanego. Z uwagi na brak ograniczenia miejsca i czasu prowadzenia kontroli (może to stanowić o naruszeniu praw i wolności kontrolowanego) wydaje się być zasadnym uwzględnienie tej kwestii, nie wyłączając przy tym możliwości przeprowadzenia kontroli w siedzibie organu.

**47. Termin zakończenia kontroli**- art. 68 projektu przewiduje konieczność zakończenia kontroli („nie może trwać dłużej niż miesiąc"). Należy wskazać, że ze względu na specyfikę kontroli oraz często bardzo szeroki zakres przedmiotu kontroli, wymóg dotyczący terminu powinien być sformułowany w inny sposób. Generalny Inspektor sugeruje wskazanie w art. 68 w ust. 1, że terminem zakończenia postępowania kontrolnego jest dzień podpisania protokołu przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 66 ust. 7. Należy również

wprowadzić zmianę w ust. 2 poprzez wskazanie, że przedłożenie protokołu do podpisania kontrolowanemu może nastąpić w terminie nie dłuższym niż miesiąc od zakończenia czynności kontrolnych.

**48. Odpowiedzialność cywilna**- jak wynika z przekazanego wcześniej wprowadzenia do projektu ustawy, art. 72 projektu ma czynić zadość określonemu w art. 79 ust. 1 rozporządzenia 2016/679 obowiązkowi zapewnienia skutecznego środka ochrony prawnej przed sądem. Projektodawca w art. 55 ust. 1, który jest pierwszym przepisem w rozdziale zatytułowanym „odpowiedzialność cywilna", przewidział wdrożenie ww. obowiązku poprzez przyznanie prawa do żądania, „ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków". Wydaje się, że art. 79 ust. 1 rozporządzenia należy interpretować w związku z art. 82 ust. 1, zgodnie z którym 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. Posłużenie się pojęciami właściwymi dla prawa cywilnego wskazuje oczywiście na drogę cywilną jako właściwą do dochodzenia odszkodowania, a zatem właściwy do rozpatrywania tych spraw będzie sąd cywilny. Wydaje się, że sformułowanie „dopełnił czynności potrzebnych do usunięcia jego skutków" niefortunnie wskazuje na możliwość zobowiązania przez sąd do podjęcia określonych czynności, podczas gdy jak się wydaje intencją prawodawcy unijnego było umożliwienie osobom, których dotyczy naruszenie, uzyskania finansowej rekompensaty w postaci odszkodowania zasądzonego przez sąd cywilny. Tak sformułowane przepisy ustawy są niejasne i powodują „pomieszanie" trybów. Możliwość wniesienia skargi do organu nadzorczego jest odrębną instytucją, której podstawowym celem jest usunięcie stanu niezgodnego z prawem, ewentualnie „ukaranie" administratora poprzez nałożenie administracyjnej kary pieniężnej. Zastosowanie tych środków może jednak w ocenie osób, których dane dotyczą, nie rekompensować im naruszeń. Proponowane brzmienie art. 55 ust. 1 może prowadzić do swoistych sporów kompetencyjnych pomiędzy organem nadzorczym a sądami powszechnymi. Projektodawca wprawdzie wyraźnie zaznaczył we wprowadzeniu do projektu, że „ani sąd powszechny ani Prezes Urzędu nie powinni być związani swoimi rozstrzygnięciami", jednak jako rozwiązanie dla takiego zagrożenia zaproponował jedynie obowiązek informowania o pierwszym rozstrzygnięciu.

Niejasne jest też dlaczego projektodawca posługuje się w tych przepisach pojęciem „organ nadzorczy". Proponuję zastosowanie jednolitych pojęć i dostosowanie brzmienia przepisów niniejszego rozdziału do języka, którym posłużono się w pozostałej części projektu, np. przeredagowanie sformułowań: „osoba, której prawa przysługujące", „ten, kto"- w rozporządzeniu 2016/679 i pozostałych przepisach zostało określone, co to za osoby.

**49. Administracyjne kary pieniężne**- wbrew wcześniej składanym deklaracjom Minister Cyfryzacji proponuje całkowite wyłączenie wobec organów publicznych (w rozumieniu art. 5 § 2 pkt 3 KPA) oraz większości podmiotów publicznych (w rozumieniu art. 9 pkt 1-7 ustawy z dnia 25 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870, z późn. zm.)) stosowania administracyjnych kar pieniężnych. Takie rozwiązanie w ocenie Generalnego Inspektora może spowodować ryzyko szerokiego wyłączenia administratorów danych spod kar administracyjnych

wobec możliwości definiowania organu publicznego w znaczeniu funkcjonalnym. Na ten problem zwróciła uwagę Komisja Ekspertów GIODO podczas posiedzenia w dniu 28 czerwca 2017 r. Równocześnie zaś w stosunku do pozostałych podmiotów publicznych ujętych w ustawie o finansach publicznych sugeruje dalsze, dziesięciokrotne, zmniejszenie maksymalnego wymiaru administracyjnej kary pieniężnej w stosunku do propozycji przedstawionej w przepisach GIODO. Zauważyć należy, iż w swojej propozycji Generalny Inspektor, w stosunku do ogółu podmiotów sektora publicznego, sugerował czterdziestokrotne zmniejszenie maksymalnego wymiaru administracyjnej kary pieniężnej w stosunku do limitów wyznaczonych przez rozporządzenie 2016/679. Tym samym, zgodnie z projektem Ministra Cyfryzacji, większość podmiotów sektora publicznego w ogóle nie będzie zagrożona administracyjnymi karami pieniężnymi, a te w stosunku do których kary będą miały zastosowanie, są zagrożone sankcją czterystukrotnie niższą od przewidzianej w rozporządzeniu 2016/679. Administracyjna kara pieniężna, przewidziana dla podmiotów publicznych, w wysokości do 100 tys. zł, w sytuacji kiedy rozporządzenie przewiduje maksymalnie 20 mln euro, jest dosyć kontrowersyjna. Zaproponowana maksymalna wysokość kary administracyjnej (100 tys. zł) dla podmiotów publicznych jest zbyt niska. Kary w zaproponowanej przez Ministra Cyfryzacji wysokości nie spełnią ani funkcji represyjnej, ani funkcji prewencyjnej. Posługując się językiem rozporządzenia, kara administracyjna w wysokości do 100 tys. zł nie będzie skuteczna, proporcjonalna i odstraszająca. W ocenie Generalnego Inspektora przyjęte rozwiązanie zakładające faktyczne ograniczenie stosowania przepisów w zakresie administracyjnych kar pieniężnych wobec sektora publicznego jest rozwiązaniem błędnym. Dotychczasowe doświadczenia wielu europejskich organów ochrony danych pokazują, że takie wyłączenia przeczą zasadzie równości wobec prawa oraz mogą wywoływać w osobach, których dane dotyczą poczucie unikania odpowiedzialności przez administratorów sektora publicznego.

Rozważając kwestię wysokości kar należy przede wszystkim zwrócić uwagę na kwestię równości podmiotów. Jaka jest bowiem różnica między szpitalem publicznym a prywatnym, w sytuacji gdy doszło w nich do wycieku danych osobowych pacjentów? Z perspektywy osób, których dane zostały utracone, sytuacja jest taka sama. I jeden, i drugi podmiot utracił władztwo nad danymi, a pacjenci ponieśli taką samą szkodę.

Zmiany wymaga zaproponowany art. 77 ust. 2 projektu, ponieważ odwołuje się wyłącznie do art. 83 ust. 2 lit. a-i i k rozporządzenia 2016/679, czyli do przesłanek i kryteriów odpowiedzialności a pomija istotne kwestie zawarte w art. 83 ust. 1 oraz ust. 3–6 rozporządzenia. Pozostawienie przepisu w zaproponowanej postaci rodzi następujące konsekwencje:

1) brak wskazania naruszeń podlegających administracyjnym karom pieniężnym;

2) brak możliwości reakcji przez organ nadzorczy w przypadku nieprzestrzegania orzeczonego nakazu poprzez nałożenie administracyjnej kary pieniężnej;

3) brak wskazania rozstrzygnięcia w sytuacji zbiegu odpowiedzialności za naruszenie kilku przepisów rozporządzenia 2016/679 i wpływu zbiegu odpowiedzialności na wysokość kary.

Projekt ustawy nie odnosi się do kwestii możliwości wielokrotnego nakładania przez organ nadzorczy administracyjnej kary w przypadku niewykonania orzeczonego nakazu. Wydaje się, że przepis w prawie krajowym dający taką możliwość organowi nadzorczemu jest jak najbardziej wskazany (potwierdza ten fakt obecna praktyka GIODO, kiedy konieczne było wielokrotne nakładanie grzywien w celu przymuszenia na zobowiązanych uporczywie uchylających się od

wykonania nakazów zawartych w decyzjach GIODO), oczywiście przy wskazaniu kwoty jakiej nie mogłyby przekroczyć wielokrotnie nakładane kary za niewykonanie orzeczonego nakazu.

Projekt nie zawiera również propozycji przepisów intertemporalnych, a są one konieczne w odniesieniu do postępowań sprawdzających wykonanie nakazów decyzji GIODO jak i wszczętych a niezakończonych postępowań egzekucyjnych.

Wracając do art. 55 projektu wskazującego, że w sprawach nieuregulowanych w ustawie stosuje się przepisy ustawy – Kodeks postępowania administracyjnego z pewnymi wyłączeniami. Kilka istotnych kwestii związanych z administracyjnymi karami pieniężnymi będzie bowiem w Kpa uregulowanych: terminy przedawnienia nakładania administracyjnej kary pieniężnej, terminy przedawnienia egzekucji administracyjnej kary pieniężnej, odsetki od zaległej administracyjnej kary pieniężnej. Jednakże zasadne wydaje się, skoro dokonano w art. 81 wyłączenia stosowania art. 189f i art. 189k k.p.a., należy dokonać również wyłączenia art. 189d k.p.a., gdyż przesłanki wymiaru kary zawarte są wprost w art. 83 rozporządzenia 2016/679.

Należy wskazać, iż projektodawca w art. 80 projektu niekonsekwentnie posługuje się pojęciami „podmiot ukarany" i „wnioskodawca".

W art. 80 ust. 7 projektu ustawy wskazano, iż „rozstrzygnięcie Prezesa Urzędu w przedmiocie odroczenia uiszczenia kary pieniężnej albo rozłożenia jej na raty następuje w drodze postanowienia, na które nie przysługuje skarga do sądu administracyjnego". Jest to zabieg niezrozumiały, gdyż zgodnie z ustawą z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2017 r. poz. 1369, 1370) „kontrola działalności administracji publicznej przez sądy administracyjne obejmuje orzekanie w sprawach skarg na: postanowienia wydane w postępowaniu administracyjnym, na które służy zażalenie albo kończące postępowanie, a także na postanowienia rozstrzygające sprawę co do istoty" (art. 3 § 2 pkt. 2). Rozstrzygnięcie w przedmiocie odroczenia uiszczenia kary pieniężnej albo rozłożenia na raty nie jest ani postanowieniem kończącym postępowanie, ani rozstrzygnięciem rozstrzygającym sprawę co do istoty. Nie przysługuje też od tego postanowienia zażalenie (projekt nie wskazuje na możliwość wniesienia zażalenia), a zatem nie jest koniecznym wskazywanie, iż od powyższego postanowienia nie przysługuje skarga do sądu administracyjnego.

**50. Przepisy karne**- W ocenie Generalnego Inspektora zasadnym jest utrzymanie w polskim systemie prawnym odpowiedzialności karnej za naruszenie przepisów o ochronie danych osobowych.

Przechodząc do szczegółowych rozważań, czyn polegający na utrudnianiu lub uniemożliwianiu przeprowadzenia czynności kontrolnych, powinien zostać zakwalifikowany jako przestępstwo, a nie – jak zaproponowano w art. 82 projektu – wykroczenie. Odpowiedzialność osoby za popełnienie wykroczenia jest dla niej o wiele mniej dolegliwa, niż ma to miejsce w przypadku przestępstwa. Istnieje zatem realne niebezpieczeństwo, iż w przypadku poważnych naruszeń zasad przetwarzania danych w danym podmiocie, dla osób zarządzających tym podmiotem bardziej opłacalne będzie ponieść konsekwencje wykroczenia polegającego na uniemożliwieniu czynności kontrolnych, aniżeli dopuścić do przeprowadzenia przez GIODO kontroli w tym podmiocie. Niezależnie od powyższego, Generalny Inspektor uważa za zasadne wprowadzenie do nowej ustawy o ochronie danych osobowych prawnych odpowiedników (z uwzględnieniem numeracji stosownych przepisów rozporządzenia 2016/679) dotychczasowych przepisów karnych z rozdziału

8 ustawy o ochronie danych osobowych, za wyjątkiem odpowiednika art. 53 obowiązującej ustawy (obowiązek rejestracji zbioru danych będzie zniesiony przez rozporządzenie 2016/679).

W ocenie Generalnego Inspektora waga niektórych naruszeń przepisów o ochronie danych osobowych przemawia za zastosowaniem wobec ich sprawców kar kryminalnych, a nie tylko środków o charakterze administracyjnym. Z dyskusji prowadzonych przez przedstawicieli GIODO z reprezentantami wymiaru sprawiedliwości wynika, iż mają oni świadomość istotności niektórych zachowań naruszających przepisy o ochronie danych osobowych i opowiadają się za utrzymaniem w nowej ustawie o ochronie danych osobowych, przepisów karnych. Nie można przy tym zapominać, iż organ nadzorczy nie uzyska z chwilą rozpoczęcia stosowania w polskim porządku prawnym rozporządzenia 2016/679 uprawnień śledczych (nie ma ich także Generalny Inspektor Ochrony Danych Osobowych). Tym samym w przypadku stwierdzenia przez organ nadzorczy faktu naruszenia przepisów o ochronie danych osobowych, a jednocześnie niemożliwości ustalenia przez ten organ odpowiedzialnego za to naruszenie, ten przypadek naruszenia przepisów o ochronie danych osobowych pozostałby w istocie bezkarny (organ nadzorczy, nie mógłby nałożyć administracyjnej kary pieniężnej nie znając odpowiedzialnego za naruszenie). Pozostawienie w nowej ustawie o ochronie danych osobowych przepisów karnych umożliwi w takiej sytuacji złożenie przez organ nadzorczy zawiadomienia o popełnieniu przestępstwa do organów ścigania, które to organy posiadają szerokie kompetencje umożliwiające ustalenie sprawców naruszeń przepisów o ochronie danych osobowych.

**51. Przepis o kadencji Generalnego Inspektora Ochrony Danych Osobowych (art.85)**- W przekazanych Ministrowi Cyfryzacji wytycznych wskazano, że art. 54 ust. 1 lit. d rozporządzenia 2016/679 należy odczytywać w ten sposób, że powołanie organu ochrony danych na gruncie nowych przepisów o ochronie danych nie może prowadzić do skrócenia kadencji osoby wcześniej pełniącej tę funkcję. Na zasadność takiego stanowiska wskazuje również wyrok TSUE w sprawie Komisja przeciwko Węgrom (C-288/12). W niniejszym wyroku Trybunał przypominał, że organy nadzorcze utworzone zgodnie z dyrektywą 95/46/WE powinny mieć możliwość wykonywania swoich zadań bez jakiegokolwiek wpływu z zewnątrz. Wymóg ten oznacza, po pierwsze, że organy te nie mogą być związane żadnymi instrukcjami w zakresie wykonywanych przez siebie funkcji oraz, po drugie, że powinny one podejmować decyzje bez jakiegokolwiek wpływu politycznego. Tymczasem dopuszczenie, aby państwo członkowskie zakończyło kadencję organu nadzorczego przed pierwotnie przewidzianym terminem bez poszanowania zasad i gwarancji uprzednio ustanowionych w tym celu we właściwych przepisach może prowadzić do posłuszeństwa tego organu względem władzy politycznej. Trybunał orzekł, że niezależność organu nadzorczego obejmuje w sposób konieczny obowiązek poszanowania kadencji owego organu i zakończenia jego kadencji z poszanowaniem właściwych przepisów.

**52. Przepisy dostosowujące, przejściowe i przepisy końcowe**-- W ocenie Generalnego Inspektora zmiany wymaga brzmienie art. 84 projektu ustawy. Proponuję następujące brzmienie tego przepisu:

„Art. 84

1. Administratorzy bezpieczeństwa informacji zarejestrowani do dnia wejścia w życie niniejszej ustawy w ogólnokrajowym, jawnym rejestrze administratorów bezpieczeństwa informacji prowadzonym na podstawie art. 46c ustawy, o której mowa w art. 99, pełnią funkcję inspektora ochrony danych w rozumieniu rozporządzenia 2016/679 pod warunkiem przekazania przez administratora danych kontaktowych inspektora ochrony danych, o których mowa w art. 4 ust 1 organowi nadzorczemu w terminie 3 miesięcy od daty wejścia w życie niniejszej ustawy.

2. Dane zawarte w ogólnokrajowym, jawnym rejestrze administratorów bezpieczeństwa informacji prowadzonym na podstawie art. 46c ustawy, o której mowa w art. 46, są udostępniane przez organ na stronie internetowej organu przez okres 3 miesięcy od daty wejścia w życie niniejszej ustawy.

3. Ust. 1 nie narusza obowiązku wyznaczenia inspektora ochrony danych określonego w art. 37 rozporządzenia 2016/679.".

W przepisie przejściowym powinno znaleźć się wyraźnie podkreślenie, że wprowadzenie możliwości kontynuowania funkcji przez dotychczasowego ABI - jeśli taka jest decyzja administratora danych - nie może być traktowane w oderwaniu od obowiązku wyznaczenia inspektora określonego w art. 37 ust. 1-4 rozporządzenia 2016/679. Funkcji, jaką pełni ten przepis rozporządzenia nie należy „osłabiać" – jest to przepis, który w istotny sposób odróżnia obecny system dobrowolnego wyznaczania ABI od systemu, w którym dla wielu podmiotów wprowadzono obowiązek wyznaczenia takiej osoby. W okresie 2 lat od wejścia w życie rozporządzenia każdy podmiot musi zatem dokonać analizy, czy w świetle rozporządzenia ma czy nie ma obowiązku wyznaczenia inspektora, i jeśli tak - zapewnić wyznaczenie takiej osoby zgodnie ze wszystkimi warunkami, jakie wynikają z przepisów rozporządzenia 2016/679.

Zatem przepis przejściowy i związane z nim wydłużenie okresu na powiadomienie o danych kontaktowych inspektora w przypadku skorzystania przez administratora danych z rozwiązania w nim przewidzianego, nie zmienia faktu, że obowiązek wyznaczenia inspektora określony w art. 37 rozporządzenia 2016/679 ciąży na administratorach i podmiotach przetwarzających od momentu stosowania rozporządzenia, tj. od 25 maja 2018 r.

Ponadto należy zauważyć że projekt Ministra Cyfryzacji nie zawiera doprecyzowania sposobu realizowania obowiązku określonego w art. 37 ust. 7 rozporządzenia 2016/679 w zakresie „publikowania danych kontaktowych inspektora ochrony danych", co może powodować uzasadnione wątpliwości podmiotów zobowiązanych co do zakresu takich danych (znaczenia tego pojęcia) i terminu realizowania tego obowiązku. Mając to na uwadze należy uzupełnić brzmienie art. 4 projektu ustawy o kolejny ustęp, w następującym brzmieniu:
„Administrator danych i podmiot przetwarzający przekazują dane kontaktowe, o których mowa w ust. 1 i 2, osobom, których dane dotyczą, poprzez ich opublikowanie na swojej stronie internetowej lub w inny, zwyczajowo przyjęty sposób, niezwłocznie po wyznaczeniu inspektora ochrony danych.".

W ocenie Generalnego Inspektora przepis art. 86 projektu ustawy jest zbędny z uwagi na to, że w przypadku zastępcy GIODO nie ma zastosowania zasada kadencyjności. Proponuję przeredagowanie art. 87 i 88 w ten sposób, że to „Biuro Generalnego Inspektora Ochrony Danych włada mieniem" i konsekwentnie „mienie staje się mieniem Urzędu".

Odnosząc się do postępowań wszczętych i niezakończonych przed dniem wejścia w życie ustawy Generalny Inspektor podtrzymuje propozycje zawarte w procedurze GIODO, przekazanej do Ministerstwa Cyfryzacji.

Odnośnie przepisów przejściowych dotyczących kontroli (art. 89 projektu ustawy) należy słowo „czynności kontrolne" zastąpić słowem „kontrola", tak aby przepis ten uzyskał następujące brzmienie: „Art. 89. Do kontroli, o których mowa w rozdziale 6, rozpoczętych przed dniem 25 maja 2018 r. stosuje się przepisy ustawy, o której mowa w art. 99."Należy wskazać, że art. 93 stanowi powtórzenie motywu 171 rozporządzenia 2016/679 i ma charakter informacyjny. Natomiast przepisy art. 94 i 97 stanowią niedopuszczalne modyfikowanie przepisów rozporządzenia 2016/679.

W odniesieniu do rejestru prowadzonego na podstawie art. 46c ustawy o ochronie danych osobowych (art. 96 projektu) nie ma potrzeby przetwarzania danych w rejestrze, w przypadku, gdyby przepis przejściowy nie był związany z administratorami bezpieczeństwa informacji wpisanymi do rejestru ABI. Art. 84 projektu ustawy posługuje się sformułowaniem „administratorzy bezpieczeństwa informacji pełniący funkcję", a zatem nie nawiązuje do zarejestrowanych ABI, tym samym nie ma konieczności dalszego przetwarzania danych w rejestrze, co powinno skutkować zastosowaniem ogólnych przepisów dotyczących archiwizacji. Natomiast gdyby przepis przejściowy dotyczył – tak jak zostało to zaproponowane przez Generalnego Inspektora - zarejestrowanych ABI, istniałaby potrzeba dalszego prowadzenia rejestru (w okresie przejściowym) oraz wprowadzenia przepisu, który stanowiłby podstawę do przetwarzania danych w rejestrze.

**Projekt wewnętrzny/roboczy**

Projekt z dnia 19 maja 2017 r.

# USTAWA

z dnia ..... 2017 r.

## o ochronie danych osobowych[1)]

### Rozdział 1

### Przepisy ogólne

**Art. 1.**1. Ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679".

2. Ustawa określa:

1) podmioty obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o wyznaczaniu;
2) zasady udzielania akredytacji i certyfikacji;
3) organ właściwy w sprawie ochrony danych osobowych;
4) postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;

---

[1)] Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 osobowych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1)

5) europejską współpracę administracyjną;
6) postępowanie kontrolne;
7) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych;
8) administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

**Art. 2.**1. Do działalności polegającej na tworzeniu oraz publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. poz. 24, z późn. zm.) a także do działalności literackiej lub artystycznej nie stosuje się przepisów art. 5 - 9 art. 11 - 22, art. 25 i 27, art. 28 ust. 3 – 10, art. 30 rozporządzenia 2016/679.

2. Do działalności akademickiej nie stosuje się przepisów art. 12 i 13, art. 15 ust. 3 i 4, art. 18, art. 25 i 27, art. 28 ust. 3 – 10, art. 30 rozporządzenia 2016/679.

***„Propozycja przepisu do nowej ustawy o ochronie danych osobowych MKiDN***

*„Art. 2. 1. Prawo do ochrony danych osobowych nie narusza wolności wypowiedzi i informacji w związku z działalnością dziennikarską, literacką lub artystyczną, chyba że wypowiedź taka istotnie narusza prawa i wolności osoby, której dane dotyczą.*

*2. Do przetwarzania danych osobowych w związku z działalnością dziennikarską, literacką lub artystyczną, nie stosuje się przepisów rozdziału II-VII oraz rozdziału IX rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, w zakresie w jakim przetwarza się dane wyłącznie w powyższych celach.".*

**Art. 3**. W przypadku usług świadczonych drogą elektroniczną oferowanych bezpośrednio osobie, która nie ukończyła lat trzynastu, gdy podstawą przetwarzania danych osobowych jest zgoda tej osoby, przetwarzanie danych osobowych możliwe jest wyłącznie po uzyskaniu uprzedniej zgody jej rodziców bądź opiekunów prawnych albo po potwierdzeniu przez rodziców lub opiekunów prawnych zgody wyrażonej przez taką osobę.

## Rozdział 2

## Inspektorzy ochrony danych

**Art. 4.** 1 Administrator danych albo podmiot przetwarzający, który wyznaczył inspektora ochrony danych, zwanego dalej „inspektorem", zawiadamia Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu". o jego wyznaczeniu, w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej albo numer telefonu inspektora.

2. W zawiadomieniu administrator danych albo podmiot przetwarzający obowiązany jest wskazać adres swojej siedziby i pełną nazwę, a w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna – miejsce zamieszkania oraz imię i nazwisko.

3. O każdej zmianie danych. o której mowa w ust. 1 i 2, należy zawiadomić Prezesa Urzędu w terminie 14 dni od dnia zaistnienia zmiany.

4. Zawiadomienia, o których mowa w ust. 1 i 3, sporządza się w postaci papierowej albo elektronicznej.

5. Prezes Urzędu prowadzi system teleinformatyczny umożliwiający przesyłanie zawiadomień w postaci elektronicznej.

6. Prezes Urzędu prowadzi ewidencję zawiadomień, o których mowa w ust. 1 i 3. Ewidencja zawiera dane, o których mowa w ust. 1 i 2.

**Art. 5**. Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora. o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się organy publiczne wskazane w art. 5 § 2 pkt 3 Kodeksu postępowania administracyjnego oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870, z późn. zm.).

## Rozdział 3

## Akredytacja i certyfikacja

**Art. 6**.1. Akredytacji, o której mowa w art. 43 rozporządzenia 2016/679, udziela Prezes Urzędu.

2. Kryteria akredytacji określa Prezes Urzędu, uwzględniając wymogi określone w art. 43 ust. 2 rozporządzenia 2016/679, i udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

**Art. 7**.1. Akredytacji dokonuje się na wniosek.

2. Wniosek o akredytację zawiera co najmniej:

1) nazwę wnioskodawcy oraz wskazanie adresu jego siedziby;

2) informacje potwierdzające spełnienie kryteriów, o których mowa w art. 6 ust. 2.

3. Do wniosku dołącza się:

1) dokumenty potwierdzające spełnienie kryteriów, o których mowa w art. 6 ust. 2 albo ich elektroniczne kopie;

2) kryteria certyfikacji opracowane przez wnioskodawcę w celu ich zatwierdzenia przez Prezesa Urzędu.

3. Wniosek składa się w postaci papierowej albo elektronicznej.

4. Prezes Urzędu rozpatruje wniosek o akredytację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia wniosku, zawiadamia wnioskodawcę o udzieleniu lub odmowie udzielenia akredytacji.

5. Zawiadamiając o udzieleniu akredytacji, Prezes Urzędu informuje wnioskodawcę o przyznaniu mu uprawnień podmiotu certyfikującego.

6. Prezes Urzędu udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej zatwierdzone kryteria certyfikacji.

7. Odmowa udzielenia akredytacji następuje w drodze decyzji w przypadku stwierdzenia, że wnioskodawca nie spełnia kryteriów, o których mowa w art. 6 ust. 2, lub w przypadku nie zatwierdzenia kryteriów certyfikacji.

8. Do decyzji, o której mowa w ust.7, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 46, 48, 51 i art. 52 ust. 2.

**Art. 8**.1. Dokumentem potwierdzającym akredytację jest certyfikat akredytacyjny.

2. Certyfikat akredytacyjny zawiera co najmniej:

1) oznaczenie organu udzielającego akredytacji i adres jego siedziby;

2) oznaczenie podmiotu certyfikującego i adres jego siedziby;

2) numer i oznaczenie certyfikatu akredytacyjnego;

3) okres, na jaki została udzielona akredytacja;

4) datę wydania i podpis Prezesa Urzędu lub osoby przez niego upoważnionej.

3. W okresie, na jaki została udzielona akredytacja podmiot certyfikujący jest obowiązany spełniać kryteria akredytacji.

4. Prezes Urzędu prowadzi wykaz podmiotów certyfikujących i udostępnia go w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

5. W przypadku, gdy podmiot certyfikujący:

1) przestał spełniać kryteria akredytacji, o których mowa w art. 6 ust. 2;

2) nie stosuje zatwierdzonych kryteriów certyfikacji;

3) podejmuje działania naruszające przepisy o ochronie danych osobowych

- Prezes Urzędu cofa udzieloną akredytację.

6. Cofnięcie akredytacji następuje w drodze decyzji.

7. Do decyzji, o której mowa w ust.6, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 46, 48. 51 i art. 52 ust. 2.

**Art. 9.**1. Prezes Urzędu w terminie, o którym mowa w art. 7 ust. 4, a także po udzieleniu akredytacji jest uprawniony do przeprowadzenia czynności sprawdzających u podmiotu certyfikującego.

2. Prezes Urzędu zawiadamia podmiot certyfikujący o zamiarze przeprowadzenia czynności sprawdzających.

3. Czynności sprawdzające przeprowadza się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze ich przeprowadzenia. Jeżeli czynności sprawdzające nie zostaną przeprowadzone w terminie 30 dni od dnia doręczenia zawiadomienia, ich przeprowadzenie wymaga ponownego zawiadomienia.

4. Czynności sprawdzające przeprowadza się na podstawie upoważnienia wydanego przez Prezesa Urzędu, które zawiera:

1) imię i nazwisko osoby przeprowadzającej czynności sprawdzające;

2) nazwę podmiotu certyfikującego;

3) zakres czynności sprawdzających.

**Art. 10**.1. Osoba przeprowadzająca czynności sprawdzające jest uprawniona do:

1) wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń;

2) wglądu do dokumentów i informacji mających bezpośredni związek z działalnością objętą akredytacją;

3) oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

4) uzyskania ustnych lub pisemnych wyjaśnień w sprawach związanych z działalnością objętą akredytacją.

2. Czynności sprawdzających dokonuje się w obecności podmiotu certyfikującego lub osoby przez niego upoważnionej.

3. Z czynności sprawdzających sporządza się protokół i przedstawia podmiotowi certyfikującemu.

**Art. 11.**1. Za czynności związane z akredytacją Prezes Urzędu pobiera opłatę w wysokości nie przekraczającej ... krotności przeciętnego miesięcznego wynagrodzenia brutto w gospodarce narodowej za ostatni kwartał.

2. Ustalając wysokość opłaty Prezes Urzędu uwzględnia w szczególności:

1) stopień skomplikowania wykonywanych czynności;

2) zakres niezbędnych do przeprowadzenia czynności sprawdzających;

3) koszt pracy jednej osoby w jednym dniu lub godzinie, pomnożony przez liczbę osób i dni lub godzin.

**Art. 12**. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, udzielają podmioty certyfikujące.

**Art. 13.**1. Certyfikacji dokonuje się na wniosek administratora lub podmiotu przetwarzającego.

2. Wniosek o certyfikację zawiera co najmniej:

1) nazwę administratora lub podmiotu przetwarzającego albo jego imię i nazwisko oraz wskazanie siedziby lub adresu zamieszkania administratora lub podmiotu przetwarzającego;

2) informacje potwierdzające spełnianie kryteriów certyfikacji.

3. Do wniosku dołącza się dokumenty potwierdzające spełnienie kryteriów certyfikacji albo ich elektroniczne kopie.

4. Wniosek składa się w postaci papierowej albo elektronicznej.

5. Podmiot certyfikujący rozpatruje wniosek o certyfikację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia wniosku, zawiadamia wnioskodawcę o udzieleniu lub odmowie udzielenia certyfikacji.

6. Odmowa certyfikacji następuje w przypadku stwierdzenia, że administrator lub podmiot przetwarzający nie spełnia kryteriów certyfikacji.

7. Podmiot certyfikujący zawiadamia administratora lub podmiot przetwarzający o odmowie udzielenia certyfikacji wskazując kryteria, których nie spełnienie było powodem odmowy.

**Art. 14**.1. Dokumentem potwierdzającym certyfikację jest certyfikat.

2. Certyfikat zawiera co najmniej:

1) oznaczenie administratora lub podmiotu przetwarzającego;
2) nazwę podmiotu certyfikującego oraz wskazanie adresu jego siedziby;
3) numer i oznaczenie certyfikatu;
4) okres, na jaki została udzielona certyfikacja;
5) datę wydania i podpis osoby uprawnionej do reprezentacji podmiotu certyfikującego.

3. W okresie, na jaki została udzielona certyfikacja administrator lub podmiot przetwarzający są obowiązani spełniać kryteria certyfikacji.

4. Podmiot certyfikujący prowadzi publicznie dostępny wykaz administratorów i podmiotów przetwarzających, którym udzielono certyfikacji.

**Art. 15**.1. Podmiot certyfikujący w terminie, o którym mowa w art. 13 ust. 5, a także po udzieleniu certyfikacji jest uprawniony do przeprowadzenia czynności sprawdzających u administratora lub podmiotu przetwarzającego w celu oceny spełniania przez ten podmiot kryteriów certyfikacji.

2. Do czynności sprawdzających stosuje się przepisy art. 9 ust. 2-4 i art. 10.

**Art. 16**.1. Podmiot certyfikujący cofa udzieloną certyfikację w przypadku stwierdzenia, że administrator lub podmiot przetwarzający przestał spełniać kryteria certyfikacji.

2. Podmiot certyfikujący zawiadamia administratora lub podmiot przetwarzający o cofnięciu certyfikacji wskazując kryteria, których nie spełnienie było powodem cofnięcia certyfikacji.

**Art. 17**.1. Podmiot certyfikujący pobiera opłatę za podjęte czynności certyfikujące w wysokości nie przekraczającej .....zł.

2. Ustalając wysokość opłaty należy uwzględnić w szczególności:

1) stopień skomplikowania wykonywanych czynności;
2) zakres niezbędnych do przeprowadzenia czynności sprawdzających;

3) koszt pracy jednej osoby w jednym dniu lub godzinie, pomnożony przez liczbę osób i dni lub godzin.

3. W przypadku cofnięcia akredytacji podmiotowi certyfikującemu, administratorowi lub podmiotowi przetwarzającemu, którzy złożyli wniosek o certyfikację przysługuje roszczenie o zwrot opłaty za czynności certyfikacyjne w całości lub w części nie znajdującej pokrycia w kosztach poniesionych przez podmiot certyfikujący.

## Rozdział 4

## Prezes Urzędu Ochrony Danych Osobowych

**Art. 18**.1. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych.

2. Prezes Urzędu jest organem nadzorczym w rozumieniu rozporządzenia 2016/679.

3. Prezesa Urzędu powołuje (*Przepis o powołaniu organu uzgadniany).*

4. Na stanowisko Prezesa Urzędu może być powołana osoba, która spełnia następujące warunki:

1) jest obywatelem polskim;

2) posiada wyższe wykształcenie prawnicze, ekonomiczne lub techniczne;

3) wyróżnia się wiedzą z zakresu ochrony danych osobowych oraz posiada co najmniej pięcioletnie doświadczenie zawodowe w obszarze związanym z ochroną danych osobowych;

4) korzysta z pełni praw publicznych;

5) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.

5. Kadencja Prezesa Urzędu trwa 4 lata od dnia jego powołania. Po upływie kadencji Prezes Urzędu pełni swoje obowiązki do czasu powołania następcy.

6. Ta sama osoba nie może być Prezesem Urzędu więcej niż przez dwie kadencje.

7. Kadencja Prezesa Urzędu wygasa z chwilą jego śmierci lub utraty obywatelstwa polskiego.

**Art. 19**. 1.(*Przepis o powoływaniu Zastępców Prezesa Urzędu uzgadniany*)

2. Na zastępcę Prezesa Urzędu może być powołana osoba, która spełnia wymogi, o których mowa w art. 18 ust. 4 pkt 1,2,4 i 5, wyróżnia się wiedzą z zakresu ochrony danych

osobowych oraz posiada co najmniej trzyletnie doświadczenie zawodowe w obszarze związanym z ochroną danych osobowych.

3. W przypadku odwołania Prezesa Urzędu jego obowiązki pełni zastępca wskazany przez ministra właściwego do spraw informatyzacji.

**Art. 21**.1. Prezes Urzędu nie może zajmować innego stanowiska, z wyjątkiem stanowiska naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, ani wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu.

2. Prezes Urzędu nie może należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.

**Art. 22**.1. Prezes Urzędu wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych, zwanego dalej „Urzędem".

2. Prezes Urzędu, w drodze zarządzenia, nadaje statut Urzędowi, określając:

1) organizację Urzędu, w tym w szczególności tworzy w Urzędzie komórkę organizacyjną do spraw rozpatrywania skarg na działalność Urzędu;

2) zakres zadań i tryb pracy komórek organizacyjnych Urzędu.

– mając na uwadze stworzenie optymalnych warunków organizacyjnych do prawidłowej realizacji zadań Urzędu.

**Art. 23**.1. Prezes Urzędu, zastępcy Prezesa Urzędu a także pracownicy Urzędu są obowiązani zachować w tajemnicy informacje, o których dowiedzieli się w związku z wykonywaniem czynności służbowych.

2. Obowiązek zachowania tajemnicy służbowej nie może być ograniczony w czasie i trwa także po zakończeniu kadencji albo zatrudnienia.

**Art. 24**.1. Przy Prezesie Urzędu działa Rada do Spraw Ochrony Danych Osobowych, zwana dalej „Radą". Rada jest organem opiniodawczo-doradczym Prezesa Urzędu.

2. Do zadań Rady należy:

1) opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych;

2) opiniowanie przekazanych przez Prezesa Urzędu projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych;3) opracowywanie propozycji kryteriów akredytacji, uwzględniających wymogi określone w art. 43 ust. 2 rozporządzenia 2016/679;

4) opracowywanie propozycji dobrych praktyk opracowywania kryteriów certyfikacji, o których mowa w art. 7 ust. 3 pkt 2; zawierających kryteria certyfikacji rekomendowane do stosowania przez podmioty certyfikujące;

5) opracowywanie propozycji rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych;

6) inicjowanie działań w obszarze ochrony danych osobowych oraz przedstawianie Prezesowi Urzędu propozycji zmian prawa w tym obszarze;

8) wyrażanie opinii w sprawach przedstawionych Radzie przez Prezesa Urzędu;

9) wykonywanie innych zadań zleconych przez Prezesa Urzędu

3. Rada wyraża opinię w terminie 21 dni od dnia otrzymania projektów lub dokumentów, o których mowa w ust. 2.

4. Opinie, protokoły posiedzeń oraz inne dokumenty Rady są udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa Urzędu.

5. Rada przedstawia Prezesowi Urzędu sprawozdanie z działalności za każdy rok kalendarzowy w terminie do dnia 31 marca następnego roku.

6. Rada składa się z 8 członków.

7. Kandydatów na członków Rady mogą rekomendować:

1) członkowie Rady Ministrów;

2) Rzecznik Praw Obywatelskich;

3) Prezes Głównego Urzędu Statystycznego;

4) Prezes Urzędu Komunikacji Elektronicznej;

5) Prezes Urzędu Ochrony Konkurencji i Konsumentów;

6) Naczelny Dyrektor Archiwów Państwowych;

7) izby gospodarcze;

8) jednostki naukowe w rozumieniu przepisów ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (Dz. U. z 2014 r., poz. 615, z późn. zm.);

9) stowarzyszenia wpisane do Krajowego Rejestru Sądowego, których celem statutowym jest działalność na rzecz ochrony danych osobowych.

8. Rekomendowany do Rady kandydat powinien posiadać wykształcenie wyższe oraz wyrazić zgodę na kandydowanie.

9. Prezes Urzędu powołuje skład Rady na dwuletnią kadencję spośród kandydatów rekomendowanych przez podmioty, o których mowa w ust. 7, w tym 4 członków spośród kandydatów rekomendowanych przez podmioty, o których mowa w ust. 7 pkt 1, 3, 6 oraz 4

członków spośród kandydatów rekomendowanych przez podmioty, o których mowa w ust. 7 pkt 2 i 7-9.

10. Przed upływem kadencji członkostwo w Radzie wygasa z powodu:

1) rezygnacji członka Rady złożonej na piśmie Przewodniczącemu Rady;

2) śmierci członka Rady;

3) niemożności sprawowania funkcji członka Rady z powodu długotrwałej choroby stwierdzonej zaświadczeniem lekarskim;

4) skazania prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.

11. W przypadkach, o których mowa w ust. 10, Prezes Urzędu powołuje na członka Rady osobę spośród pozostałych rekomendowanych kandydatów po sprawdzeniu aktualności rekomendacji.

12. Prezes Urzędu powołuje i odwołuje Przewodniczącego i Wiceprzewodniczącego Rady spośród jej członków.

13. Przewodniczący Rady kieruje jej pracami i reprezentuje ją na zewnątrz. W przypadku nieobecności Przewodniczącego zastępuje go Wiceprzewodniczący.

14. Obsługę Rady zapewnia Urząd.

15. Na posiedzenie Rady mogą być zapraszane, przez Prezesa Urzędu oraz Przewodniczącego Rady, inne osoby, o ile jest to wskazane dla realizacji zadań Rady.

16. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wysokość wynagrodzenia członka Rady za udział w posiedzeniu, uwzględniając funkcje pełnione przez członków Rady i zakres obowiązków członków Rady, a także mając na uwadze, że wynagrodzenie za jedno posiedzenie Rady nie może przekroczyć 50% minimalnego wynagrodzenia określonego na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. z 2015 r. poz. 2008, z późn. zm.), obowiązującego w dniu powołania Rady .

17. Zamiejscowym członkom Rady przysługują diety oraz zwrot kosztów podróży i zakwaterowania na warunkach określonych w przepisach wydanych na podstawie art. 775 § 2 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2016 r., poz. 1666).

18. Szczegółowy tryb działania Rady określa regulamin ustanawiany na wniosek Rady przez Prezesa Urzędu.

**Art. 25**.1. Prezes Urzędu przedstawia *(przepis o składaniu sprawozdania uzgadniany)* sprawozdanie ze swojej działalności, zawierające w szczególności informację o liczbie i

rodzaju prawomocnych orzeczeń sądowych uwzględniających skargi na decyzje lub postanowienia Prezesa Urzędu oraz wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych. Sprawozdanie za dany rok kalendarzowy składa się do dnia 31 marca roku następnego.

4. Prezes Urzędu udostępnia sprawozdanie wraz z opinią w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

**Art. 26**. Prezes Urzędu opiniuje założenia i projekty aktów prawnych dotyczące ochrony danych osobowych .

**Art. 27**.1. 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.

2. 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.

3. Podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania

**Art. 28**. Prezes Urzędu udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej:

1) standardowe klauzule umowne, o których mowa w art. 28 ust. 8 rozporządzenia 2016/679;

2) zatwierdzone kodeksy postępowania, o których mowa w art. 40 rozporządzenia 2016/679, a także zmiany tych kodeksów.

**Art. 29**. Monitorowaniem przestrzegania zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, zajmuje się podmiot akredytowany przez Prezesa Urzędu zgodnie z kryteriami określonymi w art. 41 ust. 2 rozporządzenia 2016/679.

**Art. 30**.1. Akredytacji podmiotu ubiegającego się o monitorowanie przestrzegania zatwierdzonego kodeksu postepowania dokonuje się na wniosek.

2. Wniosek o akredytację zawiera co najmniej:

1) nazwę wnioskodawcy oraz wskazanie adresu jego siedziby;

2) informacje potwierdzające spełnienie kryteriów, o których mowa w art. 41 ust. 2 rozporządzenia 2016/679.

3. Do wniosku można dołączyć dokumenty potwierdzające spełnienie kryteriów, o których mowa w art. 41 ust. 2 rozporządzenia 2016/679, albo ich elektroniczne kopie.

4. Wniosek składa się w postaci papierowej albo elektronicznej.

5. Prezes Urzędu rozpatruje wniosek o akredytację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia kompletnego wniosku, zawiadamia wnioskodawcę o udzieleniu lub odmowie udzielenia akredytacji.

6. Odmowa udzielenia akredytacji następuje w przypadku stwierdzenia, że wnioskodawca nie spełnia kryteriów, o których mowa w art. 41 ust. 2 rozporządzenia 2016/679.

**Art. 31.**1. Dokumentem potwierdzającym akredytację jest certyfikat akredytacyjny.

2. Certyfikat akredytacyjny zawiera co najmniej:

1) oznaczenie organu udzielającego akredytacji i adres jego siedziby;

2) oznaczenie podmiotu akredytowanego i adres jego siedziby;

2) numer i oznaczenie certyfikatu akredytacyjnego;

3) okres, na jaki została udzielona akredytacja;

4) datę wydania i podpis Prezesa Urzędu lub osoby przez niego upoważnionej.

3. W okresie, na jaki została udzielona akredytacja podmiot akredytowany jest obowiązany spełniać kryteria akredytacji.

4. Prezes Urzędu prowadzi wykaz podmiotów akredytowanych i udostępnia go w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

5. W przypadku, gdy podmiot akredytowany:

1) przestał spełniać kryteria akredytacji, o których mowa w art. 41 ust. 2 rozporządzenia 2016/679,

2) podejmuje działania niezgodne z przepisami rozporządzenia 2016/679

- Prezes Urzędu cofa udzieloną akredytację.

6. Prezes Urzędu zawiadamia podmiot akredytowany o cofnięciu akredytacji.

**Art. 32.** 1. Prezes Urzędu ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679.

2. Komunikat, o którym mowa w ust. 1, ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

**Art. 33**. Prezes Urzędu w procedurze uprzednich konsultacji może zawiesić bieg terminów, o których mowa w art. 36 ust. 2 rozporządzenia 2016/679, jednokrotnie i na okres nie przekraczający 14 dni.

**Art. 34.** Prezes Urzędu prowadzi system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679.

**Art. 35.**1.Prezes Urzędu w drodze decyzji:

1) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 rozporządzenia 2016/679;
2) zatwierdza kodeks postępowania, o którym mowa w art. 40 rozporządzenia 2016/679;
3) przyjmuje standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit d rozporządzenia 2016/679;
4) udziela zezwolenia, o którym mowa w art. 46 ust. 3 rozporządzenia 2016/679.

2. Do decyzji, o których mowa w ust. 1, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 46, 48, 51 i art. 52 ust. 2.

**Art. 36.**1. Prezes Urzędu opracowuje i udostępnia na swojej stronie internetowej rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.

2. Rekomendacje sporządzane są z uwzględnieniem specyfiki danego rodzaju działalności i podlegają okresowej aktualizacji.

3. Projekt rekomendacji Prezes Urzędu konsultuje z zainteresowanymi podmiotami, których zakresu działania dotyczy dany projekt.

Art. 37. Prezes Urzędu opracowuje i udostępnia na swojej stronie internetowej dobre praktyki opracowywania kryteriów certyfikacji, o których mowa w art. 7 ust. 3 pkt 2, zawierające kryteria certyfikacji rekomendowane do stosowania przez podmioty certyfikujące.

## Rozdział 4

## Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

**Art. 37.**1. Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", jest prowadzone przez Prezesa Urzędu.

2. Postępowanie jest postępowaniem jednoinstancyjnym.

**Art. 38**. Gdy prawa osoby przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, organizacja społeczna może występować z żądaniem:

1) wszczęcia postępowania,

2) dopuszczenia jej do udziału w postępowaniu,

jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes osoby, której prawa zostały naruszone.

**Art. 39**. O każdym przypadku niezałatwienia sprawy w terminie Prezes Urzędu jest obowiązany zawiadomić strony, podając przyczyny zwłoki, informację o stanie sprawy i przeprowadzonych w jej toku czynnościach oraz wskazując nowy termin załatwienia sprawy.

**Art. 40.**1. Prezes Urzędu może wyznaczyć stronie termin do przedstawienia dowodu będącego w jej posiadaniu.

2. Termin ustala się uwzględniając charakter dowodu i stan postępowania, przy czym nie może on być krótszy niż 7 dni.

3. Prezes Urzędu może żądać od strony przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę. Czynności te strona jest obowiązana wykonać na własny koszt.

**Art. 41.**1. Prawo Prezesa Urzędu do dostępu do wszelkich informacji, w tym danych osobowych, niezbędnych Prezesowi Urzędu do realizacji zadań podlega ograniczeniu ze względu na tajemnice ustawowo chronione.

2. Wykonywanie prawa, o którym mowa w ust. 1, jest możliwe na zasadach określonych w przepisach regulujących dostęp do tajemnic ustawowo chronionych.

**Art. 42.**1. Strona może zastrzec informacje, dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa, dostarczane Prezesowi Urzędu.

2. Prezes Urzędu może uchylić zastrzeżenie w drodze decyzji, jeżeli uzna, że informacje, dokumenty lub ich części nie spełniają przesłanek do objęcia ich tajemnicą przedsiębiorstwa.

3. W przypadku ustawowego obowiązku przekazania informacji lub dokumentów otrzymanych od przedsiębiorców innym krajowym lub zagranicznym organom lub instytucjom, informacje i dokumenty przekazuje się wraz z zastrzeżeniem i pod warunkiem jego przestrzegania.

**Art. 43**.1. Prezes Urzędu na wniosek lub z urzędu może, w drodze postanowienia, w niezbędnym zakresie ograniczyć prawo wglądu do materiału dowodowego, jeżeli udostępnienie tego materiału groziłoby ujawnieniem tajemnicy przedsiębiorstwa, lub innych tajemnic podlegających ochronie na podstawie odrębnych przepisów.

2. Wniosek o ograniczenie prawa wglądu do materiału dowodowego składa się do Prezesa Urzędu wraz z uzasadnieniem oraz wersją dokumentu niezawierającą informacji objętych ograniczeniem, o którym mowa w ust. 1, ze stosowną adnotacją.

3. Jeżeli wniosek nie spełnia wymagań określonych w ust. 2, Prezes Urzędu wzywa wnioskodawcę do jego uzupełnienia w wyznaczonym terminie. W przypadku nieprzedłożenia w wyznaczonym terminie wersji dokumentu, o której mowa w ust. 2, wniosek pozostawia się bez rozpoznania.

4. Stronom udostępnia się materiał dowodowy niezawierający informacji objętych ograniczeniem, o którym mowa w ust. 1, ze stosowną adnotacją.

5. Obowiązku złożenia wersji dokumentu niezawierającej informacji objętych ograniczeniem, o którym mowa w ust. 1, nie stosuje się w sytuacji gdy cały dokument jest objęty ograniczeniem, o którym mowa w ust. 1.

**Art. 44**.1. Kto, będąc obowiązany do osobistego stawienia się mimo prawidłowego wezwania nie stawił się bez uzasadnionej przyczyny jako świadek lub biegły albo bezzasadnie odmówił złożenia zeznania, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej, może być ukarany karą grzywny do 500 zł. Na postanowienie o ukaraniu służy skarga do sądu administracyjnego.

2. Prezes Urzędu na wniosek ukaranego, złożony w ciągu 7 dni od daty doręczenia postanowienia o ukaraniu, może uznać za usprawiedliwioną nieobecność lub odmowę zeznania, wydania opinii albo okazania przedmiotu oględzin i zwolnić od kary grzywny. Na postanowienie o odmowie zwolnienia od kary grzywny służy skarga do sądu administracyjnego.

**Art. 45.** W toku postępowania może być prowadzone postępowanie kontrolne, o którym mowa w rozdziale 6.

**Art. 46**.1. Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, Prezes Urzędu w celu zapobieżenia tym skutkom może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane