Materiał dotyczący koniecznych zmian legislacyjnych w zakresie statusu i kompetencji organu ochrony danych osobowych oraz w zakresie aspektów proceduralnych przepisów o ochronie danych osobowych.

Wstęp

Poniższy dokument zawiera wstępne uwagi Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej Generalnym Inspektorem lub GIODO, 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 ten nie odnosi się do innych kwestii, jak również nie wyczerpuje zagadnień, którym jest on poświęcony. Z tego względu Generalny Inspektor zastrzega sobie możliwość zgłaszania dalszych uwag i propozycji na późniejszych etapach procesu legislacyjnego.

Ze względu na charakter przedłożonego dokumentu do dużej części zagadnień odniesiono się w postaci propozycji rozwiązań kierunkowych, które w dalszym toku prac mogą zostać rozbudowane i uszczegółowione do postaci projektu legislacyjnego.

Analiza zakresu niezbędnych przepisów krajowych, które są konieczne do wdrożenia rozporządzenia 2016/679, wymaga przypomnienia, że przyjęty pakiet legislacyjny obejmuje również dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW. W trakcie procesu legislacyjnego na poziomie krajowym oba akty prawne powinny być uwzględniane równocześnie tak, aby zapewnić spójność przyszłego systemu ochrony danych osobowych w Polsce.

Kolejną kwestią, którą należy podnieść na wstępie, jest charakter prawny przyjętego przez ustawodawcę UE 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 rozporządzenia 2016/679 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 rozporządzenia 2016/679 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 niniejszego rozporządzenia do swego prawa krajowego. Niemniej należy do tej możliwości podchodzić z ostrożnością. W konsekwencji w opinii Generalnego Inspektora w polskim porządku prawnym należy przyjąć tylko takie przepisy prawa, bez których nie byłoby możliwe właściwe wdrożenie rozporządzenia 2016/679.

Należy także wspomnieć, że w pracach nad przyszłymi przepisami o ochronie danych osobowych należy także brać pod uwagę przebieg prac legislacyjnych nad nowelizacją Kodeksu postępowania administracyjnego.

Status i kompetencje organu nadzorczego

Zgodnie z art. 51 ust. 1 rozporządzenia 2016/679, każde państwo członkowskie zapewnia, by za monitorowanie stosowania rozporządzenia odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii. Każdy organ nadzorczy przyczynia się do spójnego stosowania rozporządzenia 2016/679 w całej Unii. W tym celu organy nadzorcze współpracują ze sobą i z Komisją zgodnie z rozdziałem VII (ust. 2). Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, państwo to wskazuje, który z nich ma reprezentować te organy w Europejskiej Radzie Ochrony Danych, oraz ustala mechanizm zapewniający przestrzeganie przez pozostałe organy przepisów o mechanizmie spójności, o którym mowa w art. 63 (ust. 3). Jednocześnie na mocy art. 51 ust. 4 rozporządzenia 2016/679 w terminie do 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o przepisach przyjętych na mocy rozdziału VI, a następnie niezwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

Ponadto, w myśl art. 54 ust. 1 rozporządzenia 2016/679, każde państwo członkowskie określa w swoich przepisach prawnych wszystkie poniższe elementy:

- ustanowienie każdego z organów nadzorczych;

- kwalifikacje i warunki wyboru wymagane do powołania na stanowisko członka każdego z organów nadzorczych;
- zasady i procedury powoływania członka lub członków każdego z organów nadzorczych;
- okres kadencji członka lub członków każdego z organów nadzorczych – nie krótszy niż cztery lata, z wyjątkiem pierwszej kadencji po dniu 24 maja 2016 r., która może częściowo trwać krócej, jeżeli jest to niezbędne, aby chronić niezależność organu nadzorczego w drodze procedury stopniowej wymiany członków;
- czy członek lub członkowie każdego z organów nadzorczych mogą zostać powołani ponownie, a jeżeli tak – na ile kadencji;
- zasady regulujące obowiązki członka lub członków oraz personelu każdego z organów nadzorczych, zakaz podejmowania działań, zajęć i czerpania korzyści – w trakcie kadencji oraz po jej zakończeniu – sprzecznych z tymi zobowiązaniami, a także przepisy regulujące ustanie stosunku pracy.

Odnosząc się do kształtu przyszłej krajowej regulacji w zakresie wyznaczonym przez cytowane postanowienia rozporządzenia 2016/679 poprzedzając dalsze rozważania należy wziąć pod uwagę doświadczenia związane z funkcjonowaniem dotychczasowego modelu organu ochrony danych w Polsce oraz organów w innych państwach europejskich. Przy czym należy zaznaczyć, że w Polsce organ ochrony danych osobowych działa już od przeszło 19 lat, a w niektórych krajach europejskich od ponad 40 lat. Jednocześnie w orzecznictwie Trybunału Sprawiedliwości UE został ukształtowany wysoki standard gwarancji niezależności organów ochrony danych.

Natomiast ust. 2 powołanego artykułu 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 świetle powyższego należy przychylić się do modelu jednego organu monokratycznego. Rozwiązanie takie – jak pokazują dotychczasowe doświadczenia zarówno polskie jak i zagraniczne – umożliwia większą efektywność takiego organu. Jednocześnie

biorąc pod uwagę unitarny charakter Rzeczypospolitej Polskiej trudno znaleźć argumenty za funkcjonowaniem na terytorium RP większej liczby organów ochrony danych osobowych.

Odnosząc się do potencjalnego pytania o ewentualną zmianę dotychczasowej nazwy polskiego organu ochrony danych osobowych, należy wyraźnie podkreślić, że w ocenie Generalnego Inspektora Ochrony Danych Osobowych nie stanowi to kwestii kluczowej dla procesu wdrożenia przepisów rozporządzenia 2016/679. Niemniej warto rozważyć zachowanie obecnej nazwy, gdyż niewątpliwie utrwaliła się już w świadomości administratorów danych i osób, których dane dotyczą. Podkreślenia też wymaga, że GIODO stała się już synonimem polskiego organu ochrony danych, tak jak CNIL francuskiego na forum międzynarodowym. Gdyby jednak rozważana była zmiana nazwy, to powinna ona akcentować cel i charakter działań takiego organu w obronie zasad ochrony danych, niezależnie od tego, czy naruszeń dokonuje podmiot prywatny czy publiczny. W tym kontekście można by mówić np. o Rzeczniku Ochrony Danych. Negatywnie należy natomiast oceniać ewentualne propozycje nazw jak: „Prezes Urzędu Ochrony Danych", które to urzędy co do zasady należą do administracji rządowej. Podkreślenia wymaga, że ewentualna zmiana nazwy będzie wymagała działań w celu jej promocji jako odzwierciedlenia nowego, niezależnego organu ochrony danych. Wiązałoby się to także z koniecznością zarezerwowania dodatkowych środków finansowych na potrzebę informowania społeczeństwa o zmianie nazwy.

Wydaje się też, że dotychczasowe wymogi dotyczące osoby powołanej na funkcje Generalnego Inspektora są wystarczające i mogą być zachowane. Należałoby także wprowadzić nową tajemnicę obejmującą członków organu oraz jego pracowników. Warto również rozważyć wprowadzenie wymogów, które muszą spełnić pracownicy Biura GIODO. Należałoby również utrzymać obecny związek Generalnego Inspektora z parlamentem, czego przejawem jest procedura jego powołania i odwołania przez Sejm za zgodą Senatu. Obecna długość kadencji Generalnego Inspektora spełnia minimalne wymogi określone w rozporządzeniu 2016/679. Jednakże do rozważenia jest jej wydłużenie na wzór innych organów o podobnym charakterze. Nowa ustawa powinna utrzymać zasadę, że Generalny Inspektor nie może pełnić swojej funkcji dłużej niż przez dwie kadencje. Wydaje się też, iż dotychczasowe kryteria odwołania osoby pełniącej funkcję GIODO przed końcem kadencji są zgodne z odpowiednimi postanowieniami rozporządzenia 2016/679 i mogą zostać zachowane. W tym miejscu należy zaznaczyć, 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 wcześniej pełniącej

tę funkcję. Na zasadność takiego stanowiska wskazuje również wyrok TSUE w sprawie Komisja przeciwko Węgrom (C-288/12).

W związku z tym należy zacytować art. 52 rozporządzenia 2016/679, który określa warunki niezależności organu ochrony danych. I tak: każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem działa w sposób w pełni niezależny (ust. 1). Członek lub członkowie każdego organu nadzorczego podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem pozostają wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują (ust. 2). Członek lub członkowie każdego organu nadzorczego powstrzymują się od wszelkich czynności sprzecznych ze swoimi obowiązkami i podczas swojej kadencji nie podejmują żadnego zajęcia zarobkowego ani niezarobkowego sprzecznego z tymi obowiązkami (ust. 3). Każde państwo członkowskie zapewnia, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień, w tym w zakresie wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych (ust. 4) jak również każde państwo członkowskie zapewnia, by każdy organ nadzorczy podlegał kontroli finansowej w sposób nienaruszający jego niezależności oraz dysponował odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego (ust. 6). W świetle cytowanych przepisów wydaje się, że obecne gwarancje niezależności Generalnego Inspektora zasadniczo wpisują się w ramy określone przez rozporządzenie 2016/679 i co do zasady można rozważyć ich zachowanie.

Wskazana przez ustawodawcę europejskiego konieczność zapewnienia odpowiednich zasobów organom nadzorczym niewątpliwie wiąże się z potrzebą zwiększenia środków na funkcjonowanie Biura GIODO w budżecie państwa. Bez ich zwiększenia nie będzie bowiem możliwe skuteczne wykonywanie poszerzonych zadań i uprawnień wynikających z rozporządzenia 2016/679. Niemniej wydaje się, że obecne regulacje wyodrębniające budżet GIODO i dające mu autonomię w zakresie jego zaplanowania - z perspektywy legislacyjnej - spełniają wymogi określone rozporządzeniem 2016/679.

Warto również zaznaczyć, że zgodnie z art. 52 ust. 5 rozporządzenia 2016/679, każde państwo członkowskie zapewnia, by każdy organ nadzorczy wybierał i posiadał własny personel, działający pod wyłącznym kierownictwem członka lub członków danego organu nadzorczego. Oznacza to konieczność zagwarantowania pełnej swobody Generalnemu

Inspektorowi w zakresie kadrowym. W związku z tym należy postulować, aby statut Biura GIODO był przyjmowany przez sam organ ochrony, gdyż stanowiłoby to wsparcie niezależności organu i umożliwiło bardziej swobodne kształtowanie aparatu pomocniczego, czyli Biura. Jednocześnie należy utrzymać rozwiązanie, zgodnie z którym Generalny Inspektor wykonuje swoje zadania przy pomocy Biura GIODO. Należy również postulować nadanie Generalnemu Inspektorowi kompetencji do powołania i odwołania swojego zastępcy. Jednocześnie należy zachować istniejącą obecnie możliwość tworzenia oddziałów zamiejscowych Biura GIODO.

Istotną kwestią jest również zapewnienie ciągłości prawnej pomiędzy organem ochrony danych osobowych działającym na podstawie dotychczasowych i przyszłych przepisów, co umożliwi uniknięcie różnych problemów prawnych i praktycznych, które brak takiej ciągłości mógłby powodować.

Kompetencje organu ochrony danych i kwestie proceduralne

Poprzedzając dalsze rozważania wyraźnie należy zaznaczyć, że ustawodawca europejski w rozporządzeniu 2016/679 dąży do pełnej harmonizacji kompetencji organów ochrony danych. Zakres tych kompetencji, który obejmuje: uprawnienia w zakresie postępowań, uprawnienia naprawcze, uprawnienia w zakresie wydawania zezwoleń i uprawnienia doradcze musi być w pełni nadany polskiemu organowi ochrony danych. Od strony legislacyjnej może to nastąpić poprzez odwołanie się w nowej ustawie do odpowiednich przepisów art. 58 rozporządzenia 2016/679 albo polegać na całkowitym przeniesieniu treści tych przepisów do polskiej ustawy.

W związku z zakreśleniem w rozporządzeniu 2016/679 stosunkowego katalogu spraw, co do których organy ochrony danych mają wydawać zalecenia lub wskazówki w zakresie stosowania przepisów o ochronie danych osobowych należałoby wprost nadać ogólną kompetencję Generalnemu Inspektorowi do wydawania i ogłaszania takich aktów, jak wykaz operacji określonych w art. 35 ust. 4 lub 5 rozporządzenia 2016/679, zatwierdzenie kryteriów certyfikacji, czy zatwierdzenie kryteriów akredytacji podmiotów monitorujących kodeksy postępowań. Akty te powinny być publikowane w Biuletynie Informacji Publicznej Biura.

Należy również wprowadzić obowiązek konsultacji z GIODO projektów aktów normatywnych dotyczących przetwarzania danych osobowych.

Szczególną uwagę należy zwrócić na art. 58 ust. 5 rozporządzenia 2016/679, zgodnie z którym każde państwo członkowskie przewiduje w swoich przepisach, że jego organ nadzorczy jest uprawniony do wniesienia do organów wymiaru sprawiedliwości sprawy dotyczącej naruszenia niniejszego rozporządzenia oraz w stosownych przypadkach do wszczęcia lub do uczestniczenia w inny sposób w postępowaniu sądowym w celu wyegzekwowania stosowania przepisów niniejszego rozporządzenia. Konsekwencje cytowanego przepisu dla polskiego systemu prawnego wymagają dalszej analizy, gdyż potencjalnie mogą one mieć różny charakter. Należałoby tę kompetencję organu nadzorczego przede wszystkim wiązać z rozszerzeniem na mocy art. 79 rozporządzenia 2016/679 uprawnień osób, których dane dotyczą, do dochodzenia swoich praw na drodze postępowania sądowego. Takie rozwiązanie jest novum w polskim systemie prawnym, dlatego wymaga ono jeszcze pogłębionej analizy. Wydaje się, że uprawnienie organu ochrony danych mogłoby np. polegać na kompetencji wzorowanej na kompetencji Prezesa UOKiK, który jest uprawniony do przedstawienia sądowi istotnego dla sprawy poglądu w sprawach dotyczących ochrony konkurencji i konsumentów. Art. 58 ust. 5 rozporządzenia 2016/679 może również stanowić bazę do regulacji zapewniających pełne wdrożenie orzeczenia TSUE w sprawie M. Schrems przeciwko Data Protection Commissioner w odniesieniu do kompetencji organu ochrony danych osobowych do samodzielnego wystąpienia do sądu krajowego w celu doprowadzenia do wydania przez TSUE orzeczenia prejudycjalnego w sprawie ważności decyzji Komisji Europejskie o zapewnieniu odpowiedniego poziomu ochrony danych osobowych przez państwo trzecie. Właściwym byłoby również dodanie: kompetencji do występowania do NSA i SN o podejmowanie uchwał rozstrzygających zagadnienia prawne w sprawach budzących wątpliwości w praktyce lub których stosowanie wywołało rozbieżności w orzecznictwie; prawa występowania w postępowaniu cywilnym (w sprawach dot. ochrony danych osobowych) na zasadach prokuratora; prawa składania subsydiarnych aktów oskarżenia w postępowaniu karnym, na zasadach określonych w KPK, w sprawach w których organ ds. ochrony danych osobowych składał zawiadomienia o popełnieniu przestępstwa.

Należy postulować, aby w zakresie wykonywania swoich kompetencji GIODO i pracownicy Biura GIODO mogli mieć dostęp do informacji niejawnych. Dostęp do tych informacji odbywałby się zgodnie z zasadami określonymi w przepisach o ochronie informacji niejawnych. GIODO - tak jak obecnie – miałby dostęp do takich informacji z mocy prawa, natomiast pracownicy Biura dopiero po przeprowadzeniu postępowań odpowiednich

do wskazanej klauzuli tajności. Rozważenia wymaga także określenie statusu Zastępcy GIODO w tym zakresie.

Z kwestii o charakterze horyzontalnym należy wskazać, że Generalny Inspektor negatywnie odnosi się do możliwości przewidzianej w art. 80 ust. 2 rozporządzenia 2016/679, gdyż organizacje społeczne nie powinny bez upoważnienia otrzymanego od osoby, której dane dotyczą, mieć prawa wnosić do organu nadzorczego spraw. Istnieje bowiem ryzyko nadużyć , w przypadku gdy pominięta zostanie wola osoby, która nie jest zainteresowana udziałem określonej organizacji w postępowaniu. Należałoby także mieć na uwadze przeciwdziałanie tworzeniu organizacji społecznych tylko w celu skarżenia działań podmiotów przetwarzających dane przed organami administracji i sądami.

Odnosząc się zaś do postępowań przed Generalnym Inspektorem, to należy podkreślić, że rozporządzenie 2016/679 zawiera odpowiednio wyraźne przepisy w tym zakresie, które jednak nie są kompletne. Niemniej wspomniane rozporządzenie określa m.in. terminy załatwienia spraw, bądź wykonania określonych czynności, czy w dużym zakresie określa tryb prowadzenia postępowań o charakterze transgranicznym. Nadal jednak jest pole dla regulacji krajowych określających pozostałe aspekty proceduralne.

W opinii Generalnego Inspektora prowadzone przez niego postępowania powinny się odbywać w jednej instancji z możliwością złożenia skargi do sądu administracyjnego. Odejście od dwuinstancyjności postępowania może ewentualnie być złagodzone przez mechanizm samokontroli w razie złożenia skargi do sądu administracyjnego. Niezależnie od tego koniecznym wydaje się odejście od nadzwyczajnych trybów wzruszania rozstrzygnięć. Bliższa Generalnemu Inspektorowi jest koncepcja stworzenia nowej, odrębnej procedury rozpatrywania spraw przed organem ochrony danych, podobnie jak ma to miejsce w przypadku UOKiK. Przy takim założeniu przepisy ustawy KPA stosowałoby się jedynie odpowiednio, w zakresie nieuregulowanym w procedurze przed GIODO, np. kwestie doręczeń i skuteczności, sposobu liczenia terminu, wyłączenia osób od podejmowania decyzji i czynności procesowych.

Zasadą jest, iż rozstrzygnięcia GIODO to decyzje (niezależnie od tego jak zostałyby nazwane w swojej treści). Również decyzjami byłyby nakładane administracyjne kary pieniężne zgodnie z art. 83 ust. 2 rozporządzenia 2016/679. W tym miejscu należy wskazać, że od wszystkich decyzji Generalnego Inspektora, w tym od decyzji nakładających administracyjne kary pieniężne powinna służyć skarga do sądu administracyjnego. Taki

model jest już znany polskiemu ustawodawcy, a dotychczasowa długa praktyka orzecznicza Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego dają gwarancje zapewnienia odpowiedniej fachowości w sprawach w tym zakresie.

Warto również rozważyć możliwość wszczęcia odformalizowanego postępowania wyjaśniającego, które mogłoby poprzedzić formalne wszczęcie postępowania administracyjnego.

Przepisy dotyczące właściwości (art. 55-56), współpracy (art. 60), wzajemnej pomocy (art. 61), wspólnych operacji (art. 62) oraz mechanizmu spójności (art. 63-67)

Na wstępie należy zaznaczyć, że duża część przepisów odnoszących się do działań o charakterze transgranicznym będzie stosowanych bezpośrednio, a tym samym nie będą wymagały wdrożenia w prawie polskim. Jedną z kluczowych kwestii w tym zakresie będzie określenie reżimów językowych w ramach prowadzonych działań i w odniesieniu do prowadzonej dokumentacji. Należy dopuścić możliwość prowadzenia działań w języku angielskim lub w wybranym przez organy uczestniczące w takiej procedurze języku urzędowym UE. Należy również określić zasady tłumaczenia takiej dokumentacji na język polski. Należy przyznać organowi ochrony danych kompetencję do nadania, w zakresie który mu przysługuje, uprawnień pracownikowi organu ochrony danych z innego państwa członkowskiego, który uczestniczy we wspólnej operacji na terytorium RP. Przepisy ustawowe powinny również umożliwić organowi ochrony danych określania zasad obowiązków, uprawnień i odpowiedzialności za działania w ramach wspólnych operacji w porozumieniach zawieranych przez Generalnego Inspektora i organ w niej uczestniczący.

Odnosząc się do art. 60 ust. 2 rozporządzenia 2016/679, zgodnie z którym wiodący organ nadzorczy może w dowolnym momencie zwrócić się do innych organów nadzorczych, których sprawa dotyczy, o wzajemną pomoc zgodnie z art. 61 i może prowadzić wspólne operacje zgodnie z art. 62, w szczególności w celu przeprowadzenia postępowania lub monitorowania wdrażania środka dotyczącego administratora lub podmiotu przetwarzającego posiadającego jednostkę organizacyjną w innym państwie członkowskim – wydaje się,

że doprecyzowania wymaga pojęcie „monitorowanie wdrażania środków", gdyż zapewne nie jest ono tożsame z pojęciem środków egzekucyjnych.

Odnosząc się do art. 61 ust. 8 rozporządzenia 2016/679, jeżeli organ nadzorczy nie dostarczy informacji, o których mowa w ust. 5 niniejszego artykułu, w terminie miesiąca od otrzymania wniosku innego organu nadzorczego, wzywający organ nadzorczy może zastosować środek tymczasowy na terytorium swojego państwa członkowskiego zgodnie z art. 55 ust. 1. W takiej sytuacji uznaje się, że zgodnie z art. 66 ust. 1 zachodzi pilna potrzeba działania i że zgodnie z art. 66 ust. 2 wymagana jest pilna wiążąca decyzja Europejskiej Rady Ochrony Danych. Zastanowienia wymaga charakter środka tymczasowego i możliwość jego zaskarżenia, gdyż nie wynika to z rozporządzenia. Wydaje się, że kwestia ta powinna być uregulowana na poziomie krajowym. Konieczne będzie rozstrzygnięcie jak ma wyglądać środek tymczasowy, czym ma być, czy decyzją tymczasową, cząstkową, postanowieniem? Środek tymczasowy mógłby być środkiem proceduralnym ocenianym przez sąd krajowy czy raczej jest to środek *sui generis* niezaskarżalny z uwagi na równoległe zastosowanie trybu z art. 66, który przesądza merytorycznie? Za możliwością zaskarżenia przemawia art. 78 ust. 1 RODO. Ewentualna skarga byłaby kierowana do sądu, co będzie też wymagało przyspieszenia procedury sądowo-administracyjnej.

Postępowania kontrolne

Przepisy ustawy o ochronie danych osobowych powinny zawierać szczegółowe uregulowania odnoszące się do przeprowadzania czynności kontrolnych. Należy uregulować zakres kompetencji inspektorów, sposób dokumentowania przebiegu kontroli, przeprowadzania czynności dowodowych, procedury przeprowadzania kontroli, a także udziału w czynnościach kontrolnych pracowników innych organów ochrony danych oraz osób dysponujących wiadomościami specjalnymi. Należy również nadać inspektorom kompetencję do korzystania z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji, które wykonują czynności na polecenie inspektorów.

Należy w ustawie o swobodzie działalności gospodarczej (w obecnym art. 77) wprowadzić przepis wskazujący, iż obecnego rozdziału 5 („Kontrola działalności gospodarczej przedsiębiorcy") nie stosuje się do kontroli przedsiębiorcy w zakresie przestrzegania przepisów o ochronie danych osobowych.

Uprzednie konsultacje

W odniesieniu do procedury uprzednich konsultacji należy postulować by w przyszłej ustawie o ochronie danych osobowych wprowadzić obowiązek prowadzenia komunikacji drogą elektroniczną, przy wykorzystaniu pomocniczego formularza zapewnionego przez organ ochrony danych osobowych, który także powinien zapewnić odpowiednie rozwiązania informatyczne. Należy podkreślić, że pisemne zalecenie nie będzie miało charakteru wiążącego, natomiast taki charakter może mieć skorzystanie z uprawnień określonych w art. 58 rozporządzenia 2016/679. Należy dopuścić sytuację, w której pisemne zalecenie poprzedzi wydanie aktu określonego w art. 58.

Zgłaszanie naruszeń ochrony danych

W odniesieniu do zgłaszania naruszeń ochrony danych należy postulować wprowadzenie ich zgłaszania drogą elektroniczną przy wykorzystaniu pomocniczego formularza przygotowanego przez organ ochrony danych osobowych. Przepisy ustawy o ochronie danych osobowych powinny również wskazywać, że organ ochrony danych osobowych zapewnia w tym celu odpowiednie rozwiązania informatyczne.

Zawiadamianie organu nadzorczego o danych kontaktowych inspektora ochrony danych

Zgodnie z art. 37 ust. 7 rozporządzenia 2016/679, administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Należy zauważyć, że powołany przepis nie wprowadza obowiązku rejestracji inspektorów ochrony danych ani prowadzenia ich jawnego rejestru przez organ ochrony danych. Ustawodawca europejski skoncentrował się na publikowaniu danych kontaktowych przez administratora danych i podmiot przetwarzający. Należy jedynie zawiadomić o danych kontaktowych inspektora organ ochrony danych osobowych, z czym nie wiążą się jakiekolwiek skutki prawne. Dlatego należy uznać, że zgłoszenie takich danych nie przewiduje konieczności prowadzenia rejestru. Należy raczej uznać, że organ ochrony danych w takich sytuacjach będzie prowadził wewnętrzną ewidencję o charakterze pomocniczym.

W planowanej ustawie należałoby określić tryb zawiadamiania o danych kontaktowych. Powiadomienie powinno następować zarówno po wyznaczeniu inspektora, jak i w przypadku zmiany osoby na tym stanowisku oraz w przypadku zmiany jej danych kontaktowych. W przeciwnym razie, nie będzie jasnego przepisu zapewniającego organowi nadzorczemu posiadanie aktualnych danych inspektora ochrony danych. Wydaje się, że zawiadomienie powinno nastąpić w terminie 30 dni od dnia wyznaczenia inspektora ochrony danych (można rozważyć krótszy termin). Sam proces zawiadomienia powinien nastąpić drogą elektroniczną na formularzu pomocniczym, który ma być zapewniony przez organ ochrony danych osobowych. Ustawodawca powinien doprecyzować informacje określone jako dane kontaktowe. Formularz powinien obejmować również dane identyfikujące administratora danych. Dodatkowe może wprowadzić możliwość podawania danych fakultatywnych, takich jak imię i nazwisko inspektora ochrony danych. Ponieważ mamy do czynienia z elektroniczną formą dopełnienia obowiązku ustawowego, warto również zastanowić się nad sposobem identyfikacji osoby, która wprowadza dane do formularza, co wyeliminuje przypadki nieuprawnionych czy fałszywych powiadomień.

Kodeksy postępowania

Na wniosek zainteresowanych podmiotów organ nadzorczy wydaje opinię o zgodności projektu kodeksu, zmiany lub rozszerzenia z niniejszym rozporządzeniem i zatwierdza taki projekt kodeksu, zmiany lub rozszerzenia, jeżeli uzna, że stanowią one odpowiednie zabezpieczenia. Zatwierdzenie kodeksu itp. będzie odbywało się w formie decyzji administracyjnej. Przepisy projektowanej ustawy powinny określać tryb prowadzenia rejestru zatwierdzonych kodeksów oraz określać, że taki kodeks ma być opublikowany na stronie BIP Biura GIODO.

Ustawa o ochronie danych powinna nadać organowi ochrony danych kompetencję do wydawania akredytacji podmiotów monitorujących zatwierdzone kodeksy postępowania określając tryb takiej procedury. Analogicznie należy określić formę przyjęcia kryteriów akredytacji.

Certyfikacja w zakresie ochrony danych osobowych

Artykuł 42 ogólnego rozporządzenia o ochronie danych wprowadza możliwość ustanowienia mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych. Certyfikacja ma być dobrowolna i ma świadczyć o zgodności z ww. rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające.

Certyfikacja ma być wykonywana przez organy nadzorcze lub przez podmioty certyfikujące określone w art. 43 ogólnego rozporządzenia o ochronie danych. W związku z tym proponuje się, aby ustawodawca dopuścił wykonywanie certyfikacji zarówno przez organ nadzorczy, jak i przez akredytowane podmioty certyfikujące. Obecnie w Polsce certyfikacji w zakresie ochrony danych osobowych nie wykonuje ani GIODO, ani inne podmioty certyfikujące, które natomiast wykonują certyfikację np. w zakresie zarządzania informacją, czy bezpieczeństwem informacji. Jednakże analiza porównawcza pokazuje przykłady certyfikacji wykonywanej przez organy nadzorcze oraz podmioty certyfikujące. Takie rozwiązanie może umożliwić zaoferowanie na rynku szerokiego spektrum mechanizmów certyfikacji, znaków jakości i oznaczeń w zakresie ochrony danych osobowych. Należy zatem postulować wykonywanie certyfikacji zarówno przez organ ochrony danych, jak i podmioty certyfikacyjne.

Kryteria certyfikacji zatwierdza organ nadzorczy lub Europejska Rada Ochrony Danych. W przypadku, gdy kryteria są zatwierdzane przez Europejską Radę Ochrony Danych, może to skutkować wspólną certyfikacją, europejskim znakiem jakości ochrony danych. Z tego względu przyszła ustawa o ochronie danych osobowych powinna przyznać taką kompetencję organowi nadzorczemu.

W obszarze dotyczącym zarządzania ochroną danych osobowych, najbardziej zbliżonym systemem akredytacji i certyfikacji obecnie funkcjonującym w Polsce jest certyfikacja systemu zarządzania na zgodność z normą ISO/IEC 27001. Akredytacje w tym zakresie podmiotom certyfikującym wydaje Polskie Centrum Akredytacji, wymagania dla podmiotów certyfikujących (kryteria akredytacji określa norma ISO.IEC 27006), kryteria certyfikacji określa norma ISO/IEC 27001.

Analizy wymagałoby także:

1) opracowanie kryteriów i warunków jakie musi spełniać jednostka organizacyjna Biura GIODO oraz podmiotu certyfikacyjnego upoważnione do przeprowadzania audytów certyfikujących.

2) opracowanie kryteriów certyfikacji oraz sposobów ich weryfikacji, oraz

3) opracowanie procedur przeprowadzania procesu certyfikacji (wniosek, audyt certyfikacyjny, ocena wyników, wydanie certyfikatu, weryfikacja)

Jednakże wydaje się, że ustawa powinna określać kompetencje do wydawania ww. dokumentów.

Rozporządzenie 2016/679 wprowadza również mechanizm akredytacji podmiotów certyfikacyjnych. Podmiot certyfikujący, to podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych. Zgodnie z art. 43 ust. 1 rozporządzenia 2016/679, akredytacja podmiotów certyfikujących ma być wykonywana przez: organ nadzorczy lub krajową jednostkę akredytującą (w Polsce jest to Polskie Centrum Akredytacji).

Kryteria akredytacji zatwierdza GIODO lub Europejska Rada Ochrony Danych. Wymagania co do krajowej jednostki akredytującej określa rozporządzenie Parlamentu Europejskiego i Rady nr 765/2008. Dodatkowe wymagania może także określić GIODO. Zgodnie z ww. rozporządzeniem:

- „akredytacja" oznacza poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych konieczne do realizacji określonych czynności związanych z oceną zgodności;
- „krajowa jednostka akredytująca" oznacza jedyną autorytatywną jednostkę w państwie członkowskim, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo.

Akredytacja Podmiotów certyfikujących wykonywana byłaby zaś przez organ ochrony danych osobowych, który jednak mógłby zlecić wykonywanie tego zadania przez PCA, która zostało wskazane w Ustawie z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku jako jedyna krajowa jednostka akredytującą.

Jednocześnie należy nadać Ministrowi ds. informatyzacji delegację do wydania rozporządzenia wykonawczego określającego odpłatnosc za czynności związane z certyfikacją i akredytacją.

Administracyjne kary pieniężne

Generalny Inspektor popiera rozszerzenie zakresu podmiotowego na podmioty publiczne, gdyż również w odniesieniu do sektora publicznego ten instrument zapewniłby wyższy poziom zgodności. Kryteria nakładania kar powinny być wzorowane na treści art. 83 rozporządzenia 2016/679, aczkolwiek z możliwymi modyfikacjami uwzględniającymi specyfikę sektora publicznego. Generalnie w zakresie nakładania administracyjnych kar pieniężnych należy przyjąć, że adresat takiego nakazu będzie mógł złożyć skargę do sądu administracyjnego. Jednocześnie należy określić metodę wyrażania (przeliczania) wysokości kary w walucie polskiej (PLN).. Ponadto, należy wskazać, że do takich należności stosuje się przepisy o egzekucji w administracji oraz ewentualnie wskazać właściwy organ egzekucyjny.

Proponowane przepisy przejściowe.

W związku z rezygnacją przez ustawodawcę unijnego z obowiązków zgłaszania operacji przetwarzania danych oraz tzw. kontroli wstępnej, które w polskim systemie prawnym zostały wdrożone jako obowiązek zgłaszania zbiorów danych osobowych do ogólnokrajowego, jawnego rejestru zbiorów danych osobowych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych, kwestią wymagającą uregulowania w przepisach przejściowych jest określenie sposobu i trybu zakończenia postępowań w sprawach wszczętych i niezakończonych do dnia 25 maja 2018 r., a dotyczących: zgłoszenia zbioru do rejestracji (art. 40), zgłoszenia zmian w zbiorze (art. 41 ust. 2), wydania zaświadczeń o zarejestrowaniu zbioru na wniosek administratora danych (art. 42 ust. 3), wydania decyzji o odmowie rejestracji zbioru danych (art. 44 ust. 1), wydania decyzji o wykreśleniu zbioru z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych (art. 44a).

Z datą rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych nie będzie już materialnoprawnych podstaw do prowadzenia ww. postępowań, a tym samym postępowania niezakończone przed 25 maja 2018 r. z powodu swojej bezprzedmiotowości będą wymagały umorzenia. Ze względu na potencjalnie dużą liczbę takich spraw należałoby postulować wprowadzenie do mającej powstać regulacji normatywnej z zakresu ochrony danych osobowych o randze ustawy przepisu przejściowego umarzającego ww. postępowania z mocy prawa. Przykładem zastosowania takiego rozwiązania przez

ustawodawcę są: art. 204 ust. 4 pkt. 1 ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej. (t.j. Dz. U. z 2015 r. poz. 618 z późn. zm.); art. 6 ust 1 ustawa o uchyleniu ustawy o wyrobach stosowanych w medycynie weterynaryjnej oraz o zmianie innych ustaw (Dz. U. z 2010 r. Nr 78, poz. 513); art. 170 ust. 1 ustawy Prawo restrukturyzacyjne (Dz. U. z 2015 r. poz. 978.)

W związku z odstąpieniem przez ustawodawcę unijnego od rozwiązań przyjętych w art. 46b i następnych ustawy o ochronie danych osobowych, które przewidują procedurę rejestracji administratorów bezpieczeństwa informacji, i zastąpienie ich zgłoszeniem organowi nadzorczemu danych kontaktowych inspektora ochrony danych, należy również postulować umorzenie z mocy prawa niezakończonych przez 25 maja 2018 r. postępowań związanych ze ze zgłoszeniem powołania i odwołania ABI oraz aktualizacji informacji zawartych w zgłoszeniu oraz postępowań o wydanie zaświadczenia o zarejestrowaniu ABI, a także ewentualnych postępowań w sprawie wykreślenia ABI z rejestru..

Podkreślenia wymaga, że pełnienie funkcji przez inspektora ochrony danych, który zastąpi obecnego administratora bezpieczeństwa informacji nie będzie już powiązane z wpisem do rejestru. Co więcej – jak już wczesnej wskazano – ogólne rozporządzenie o ochronie danych nie przewiduje obowiązku prowadzenia przez organy nadzorcze jakiegokolwiek jawnego rejestru inspektorów ochrony danych.

W związku ze zmianą nazwy obecnych administratorów bezpieczeństwa informacji na inspektorów ochrony danych oraz w pewnym zakresie zmianą ich statusu i zakresu kompetencji, a także faktem, że obecny status i kompetencje administratorów bezpieczeństwa informacji, który obowiązuje od 1 stycznia 2015 r., miał na celu przygotowanie tej grupy osób do wymogów określonych ogólnym rozporządzeniem o ochronie danych, jak również związanej z tym postępującej profesjonalizacji osób pełniących tę funkcję, proponowane jest wprowadzenie przepisów przejściowych, zgodnie z którymi administratorzy bezpieczeństwa informacji zarejestrowani w ogólnokrajowym, jawnym rejestrze administratorów bezpieczeństwa informacji przed 25 maja 2018 r. z mocy prawa stają się inspektorami ochrony danych. Takie rozwiązanie powoduje, że administratorzy bezpieczeństwa informacji, którzy spełnili wszystkie obecnie wymagane kryteria, aby pełnić swoją funkcję będą mogli dalej ją pełnić bez konieczności podejmowania w tym zakresie przez administratorów danych dodatkowych formalnych czynności. Takie rozwiązanie odpowiada na postulaty zgłaszane przez interesariuszy i w żaden sposób nie ogranicza kompetencji administratorów danych. Należy także nadmienić, że obecnie powołanie administratora bezpieczeństwa informacji jest w pełni dobrowolne, a w przyszłym modelu wyznaczenie inspektora ochrony danych w części

będzie obowiązkowe. W konsekwencji nie można wykluczyć stosunkowo dużej grupy inspektorów ochrony danych, których wyznaczenie będzie obowiązkowe, gdy dotąd było to fakultatywne.

Od kwestii dotyczących statusu obecnych administratorów bezpieczeństwa informacji na gruncie przepisów ogólnego rozporządzenia o ochronie danych należy odróżnić nowy obowiązek zawiadomienia organu nadzorczego o danych kontaktowych inspektora ochrony danych (art. 37 ust. 7 ogólnego rozporządzenia). Obowiązek ten swoim zakresem oraz charakterem prawnym istotnie odróżnia się od obecnego mechanizmu rejestracji administratorów bezpieczeństwa informacji. Z tego względu należy przyjąć, że administratorzy danych lub podmioty przetwarzające mają odrębnie spełnić ten obowiązek również w odniesieniu do dotychczasowych administratorów bezpieczeństwa informacji, którzy z mocy prawa stali się inspektorami ochrony danych. Jednakże należy wprowadzić przepis przejściowy, zgodnie z którym w odniesieniu do inspektorów ochrony danych, którymi z mocy prawa stali się dotychczasowi administratorzy bezpieczeństwa informacji, obowiązek zawiadomienia o danych kontaktowych należy zrealizować w terminie sześciu miesięcy od dnia rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych (niemniej można rozważyć skrócenie tego terminu).

Podkreślenia wymaga, że w odniesieniu do obu ogólnokrajowych, jawnych rejestrów od 25 maja 2018 r. nie będzie już podstaw prawnych do ich prowadzenia przez Generalnego Inspektora, a co za tym idzie dane z tych rejestrów nie będą już dłużej ujawniane, zaś dane w nich zawarte jak i akta rejestrowe będą podlegały archiwizacji. Nie wydaje się by w tym zakresie istniała konieczność wprowadzenia odrębnych przepisów, gdyż obowiązujące w tym zakresie zasady ogólne powinny być wystarczające.