GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak - Jomaa

Warszawa, dnia 14 maja 2018 r.

DOLiS-023-422/17/TG-/8201/18

Pan

Robert Mamątow

Senator

Rzeczypospolitej Polskiej

Przewodniczący Komisji Praw Człowieka,

Praworządności i Petycji

Senat

Rzeczypospolitej Polskiej

ul. Wiejska 6

00 – 902 Warszawa

Wielce Szanowny Panie Przewodniczący,

w związku ze skierowaniem do Senatu Rzeczypospolitej Polskiej, uchwalonej przez Sejm Rzeczypospolitej Polskiej, **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**, zwracam uwagę, że zakończenie procesu legislacyjnego dotyczącego tej ustawy tak, by weszła ona w życie w dniu 25 maja 2018 r., pozwoli na dostosowanie krajowego porządku prawnego do stosowania 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)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1), powoływanego dalej z zastosowaniem skrótu „rozporządzenie 2016/679". Nieprzyjęcie przez ustawodawcę krajowego **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**

ul. Stawki 2
00-193 Warszawa

tel. 22 531 03 88
fax. 22 531 03 99

nie wpłynie na wstrzymanie stosowania rozporządzenia 2016/679 w Rzeczypospolitej Polskiej, jednak może utrudnić sprawne funkcjonowanie organu nadzorczego oraz negatywnie oddziaływać na sposób realizacji przez ten organ obowiązków nałożonych rozporządzeniem 2016/679. Biorąc to pod uwagę, Generalny Inspektor Ochrony Danych Osobowych zwraca się z uprzejmą prośbą o uwzględnienie tych okoliczności w pracach Senatu Rzeczypospolitej Polskiej dotyczących **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**.

Jednocześnie Generalny Inspektor Ochrony Danych Osobowych – jako niezależny i wyspecjalizowany organ nadzorczy ds. ochrony danych osobowych, funkcjonujący w polskim porządku prawnym już ponad 20 lat – aktywnie podejmuje działania zmierzające do zapewnienia spójności przyszłego systemu ochrony danych osobowych w Polsce z założeniami unijnej reformy ochrony danych oraz przeciwdziała próbom obniżania poziomu ochrony danych osobowych w stosunku do dotychczasowych standardów. Przekazane do Senatu Rzeczypospolitej Polskiej przepisy **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** budzą nadal szereg poważnych wątpliwości, na które Generalny Inspektor Ochrony Danych Osobowych zwracał wielokrotnie uwagę w toku prowadzonego procesu legislacyjnego. W związku z powyższym przekazuję uwagi Generalnego Inspektora Ochrony Danych Osobowych do, uchwalonej przez Sejm Rzeczypospolitej Polskiej, **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**.

Nazwa organu ochrony danych osobowych. Generalny Inspektor Ochrony Danych Osobowych niezmiennie podtrzymuje uwagę dotyczącą niezasadności zmiany nazwy polskiego organu ochrony danych osobowych i zastąpienia Generalnego Inspektora Ochrony Danych Osobowych Prezesem Urzędu Ochrony Danych Osobowych. Od samego początku Generalny Inspektor Ochrony Danych Osobowych podkreślał, że sama zmiana nazwy organu nadzorczego nie jest kwestią kluczową pośród wielu innych elementów wdrożenia w Rzeczypospolitej Polskiej rozporządzenia 2016/679. Niemniej jednak Generalny Inspektor Ochrony Danych Osobowych podtrzymuje swoje stanowisko, że żaden z przepisów tego rozporządzenia nie wymaga takiej zmiany, a taką propozycję uznać należy za niepotrzebną i kosztowną. Wyniki badania opinii publicznej „Wiedza i opinie polskich przedsiębiorców na temat zmian prawnych w zakresie ochrony danych osobowych", które w grudniu 2017 r. na zlecenie Generalnego Inspektora Ochrony Danych Osobowych przeprowadził Kantar Public, to potwierdzają. Wśród wielu pytań znalazło się to o znajomość organu nadzorującego w Polsce przestrzeganie przepisów z zakresu ochrony danych osobowych. Aż 84% badanych potrafiło spontanicznie wskazać GIODO jako ten organ. Należy więc postawić pytanie

o koszty społeczne zmiany nazwy organu ochrony danych osobowych w Polsce, związane z utrwalaniem w społecznej świadomości nowej nazwy rozpoznawalnego już GIODO. Spowoduje to również duże, niepotrzebne, utrudnienia organizacyjne.

Biorąc też pod uwagę to, że uzyskanie przez organ ochrony danych osobowych środków finansowych niezbędnych na przygotowanie urzędu do stosowania rozporządzenia 2016/679 jest opóźnione, wypada zastanowić się, czy rzeczywiście zasadne jest dodatkowe ponoszenie kosztów związanych ze zmianą nazwy organu.

Ograniczenie prawa do informacji osób, których dane dotyczą (art. 5). Projektodawca w art. 5 ust. 2 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** wprowadził daleko idący wyjątek od stosowania art. 15 ust. 1 i 3 rozporządzenia 2016/679. Komentowany przepis ustawy przewiduje nałożenie obowiązku na osobę, której dane dotyczą, udzielenia informacji pozwalających na wyszukanie przez administratora jej danych w przypadkach, gdy samodzielne wyszukanie danych przez administratora będzie wymagało niewspółmiernie dużego wysiłku. Przesłanka „niewspółmiernie dużego wysiłku" nie wynika z art. 12 rozporządzenia 2016/679 i nie znajduje oparcia w art. 15 rozporządzenia 2016/679. Przyjęcie takiego rozwiązania nie spełnia również wymagań określonych w art. 23 rozporządzenia 2016/679. W związku z powyższym należy je uznać niezgodne z rozporządzeniem 2016/679.

Wyłączenie stosowania rozporządzenia 2016/679 w stosunku do działalności służb specjalnych w rozumieniu art. 11 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Wywiadu (art. 6 pkt 2). Na etapie rozpatrywania projektu ustawy przez Radę Ministrów został dodany art. 6 pkt 2, na podstawie którego rozporządzenie 2016/679 nie będzie stosowane do służb specjalnych: Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego. W ocenie Generalnego Inspektora Ochrony Danych Osobowych zaproponowane wyłączenie jest niezgodne z przepisami rozporządzenia 2016/679. Art. 2 rozporządzenia 2016/679 określa przedmiotowy zakres zastosowania rozporządzenia, natomiast w art. 2 ust. 2 określone zostały wyłączenia z zakresu przedmiotowego jego zastosowania. Wyłączenia obejmują przetwarzanie danych:

1) w ramach działalności nieobjętej zakresem prawa Unii;

2) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

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

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

Niestety zaproponowane brzmienie art. 6 pkt 2 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** nie ogranicza się tylko do działalności służb specjalnych nieobjętej prawem Unii Europejskiej. Nie należy zapominać, że każda z wymienionych służb specjalnych realizuje zadania związane ze służbą funkcjonariuszy (zatrudnieniem pracowników). Realizacja tego zadania nie podlega wyłączeniu i niedopuszczalne jest, aby w tym zakresie zostało wyłączone stosowanie rozporządzenia 2016/679.

W dalszym ciągu Generalny Inspektor Ochrony Danych Osobowych podtrzymuje stanowisko wyrażone w opinii GIODO skierowanej na etapie prac Stałego Komitetu Rady Ministrów oraz Rady Ministrów, zgodnie z którym – w świetle motywu 16 i brzmienia art. 2 lit. a rozporządzenia 2016/679 – zbędny jest art. 6 pkt 1 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**, gdyż stanowi powtórzenie przepisu rozporządzenia 2016/679.

W świetle powyższych rozważań zasadnym byłoby usunięcie całego art. 6 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**.

Dodatkowe uprawnienia organu i kwestia rozstrzygania sporów o właściwość. Generalny Inspektor Ochrony Danych Osobowych zgłaszał na wcześniejszych etapach prac legislacyjnych uwagę co do konieczności wyposażenia organu nadzorczego w dodatkowe uprawnienia, takie jak uprawnienie do występowania z wnioskiem do Sądu Najwyższego o rozstrzygnięcie zagadnienia prawnego, jeżeli w orzecznictwie sądów powszechnych ujawnią się rozbieżności w wykładni przepisów prawa dotyczących ochrony danych osobowych, oraz uprawnienie do złożenia wniosku do Naczelnego Sądu Administracyjnego o podjęcie uchwały mającej na celu wyjaśnienie przepisów prawnych, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych. Generalny Inspektor Ochrony Danych Osobowych proponuje wprowadzenie do **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** przepisu o następującym brzmieniu:

„Art. ..... Generalny Inspektor/Prezes Urzędu/, w zakresie swojej właściwości, może:

1) występować z wnioskiem do Sądu Najwyższego o rozstrzygnięcie zagadnienia prawnego, jeżeli w orzecznictwie sądów powszechnych

ujawnią się rozbieżności w wykładni przepisów prawa dotyczących ochrony danych osobowych;

2) występować z wnioskiem do Naczelnego Sądu Administracyjnego o podjęcie uchwały mającej na celu wyjaśnienie przepisów prawnych, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych."

Zaproponowana zmiana będzie wymagała również nowelizacji art. 83 §2 ustawy z dnia 8 grudnia 2017 r. o Sądzie Najwyższym oraz art. 264 § 2 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi.

Jednocześnie aktualna pozostaje uwaga Generalnego Inspektora Ochrony Danych Osobowych dotyczącą konieczności wprowadzenia do **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** przepisów dotyczących rozstrzygania sporów kompetencyjnych między niezależnym organem nadzorczym a innymi organami administracji publicznej.

Rada do Spraw Ochrony Danych Osobowych (art. 48). Generalny Inspektor Ochrony Danych Osobowych podtrzymuje uwagę dotyczącą niezasadności powołania Rady do Spraw Ochrony Danych Osobowych w zaproponowanym kształcie. Z zaproponowanego brzmienia art. 48 projektu **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** nie wynika: czy powołana Rada ma być niezależna od Prezesa Urzędu i samodzielnie wykonywać – wskazane w **ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych** – zadania, 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 art. 48 ust. 2 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** zakres zadań Rady podważa kompetencje Prezesa Urzędu i jednocześnie przeczy założeniom określonym w ust. 1, zgodnie z którymi jest ona „organem opiniodawczo-doradczym" Prezesa Urzędu. Jednocześnie należy zastanowić się, czy naruszeniem rozporządzenia 2016/679 nie będzie to, że „osoby reprezentujące różne podmioty, zarówno ze strony administracji publicznej, jak i spoza administracji" będą opiniowały projekty dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych oraz opracowywały propozycje kryteriów certyfikacji.

Należy po raz kolejny podnieść, że organ nadzorczy ma działać w sposób niezależny, a przedstawiony zakres zadań Rady oraz ewentualny skład Rady może budzić wątpliwości co do możliwości wywieranie przez tę Radę nacisku na Prezesa Urzędu.

Generalny Inspektor Ochrony Danych Osobowych nie sprzeciwia się idei funkcjonowania ciała doradczego przy organie nadzorczym. Pomysł ten nie jest przy tym rozwiązaniem nowym, przez wiele lat przy GIODO funkcjonowała Rada Naukowa. Obecnie Generalny Inspektor Ochrony Danych Osobowych 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 osobowych przy poszanowaniu zasady, że Generalny Inspektor Ochrony Danych Osobowych nie jest związany żadnymi opiniami i wytycznymi przygotowanymi przez te zespoły. Generalny Inspektor Ochrony Danych Osobowych nie widzi potrzeby uregulowania w przepisach ustawy kwestii istnienia jednostki pomocniczo-doradczej, jej funkcjonowania i zadań. Za wystarczające należałoby uznać pozostawienie tej kwestii do uregulowania w statucie organu nadzorczego. W takim przypadku przepis art. 48 powinien wskazywać jedynie na możliwość powołania przez Prezesa Urzędu Rady do Spraw Ochrony Danych Osobowych oraz na uprawnienie Prezesa Urzędu do samodzielnego określania zakresu zadań Rady i wyboru jej członków w drodze aktu wewnętrznego.

Generalny Inspektor Ochrony Danych Osobowych wskazywał, że niezrozumiałe jest dlaczego ustawodawca w art. 48 ust. 9 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** umożliwił zwolnienie członka Rady z zachowania tajemnicy w odniesieniu do informacji, o których członek Rady dowiedział się w związku z wykonywaniem swojej funkcji (szczególnie jeśli uwzględnić, iż możliwości takiej nie przewidziano w stosunku do pracowników organu nadzorczego). Jednocześnie w **ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych** nie znalazł się przepis przewidujący konsekwencje dla członka Rady w przypadku naruszenia tej tajemnicy (nie jest to przesłanka do odwołania członka Rady, a nie jest on pracownikiem organu nadzorczego, więc nie będzie można wobec niego wyciągnąć konsekwencji służbowych). Wreszcie, art. 48 ust. 9 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** nie obejmuje swoim zakresem osób zaproszonych na posiedzenie Rady, o których mowa w art. 48 ust. 16 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**. Rodzi to zasadnicze wątpliwości czy osoby te są zobowiązane do zachowania w tajemnicy informacji, o których dowiedziały się na posiedzeniu Rady, w którym uczestniczyły.

W kontekście wynagradzania członków Rady za udział w posiedzeniu należy wskazać, że GIODO stoi na stanowisku, iż członkom Rady nie powinno przysługiwać wynagrodzenie

za udział w jej pracach. Przyznawanie wynagrodzeń członkom Rady będzie generowało dodatkowe, niepotrzebne, koszty dla funkcjonowania organu nadzorczego.

Nieuzasadnione rozszerzenie katalogu podmiotów, które będą mogły wystąpić z wnioskiem o przeprowadzenie uprzednich konsultacji (art. 57 ust. 1).

Treść art. 57 ust. 1 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** została zmieniona na etapie prac Komisji Prawniczej poprzez wskazanie, że z wnioskiem o przeprowadzenie uprzednich konsultacji może wystąpić administrator lub podmiot przetwarzający. Należy podkreślić, że zgodnie z art. 36 ust. 1 rozporządzenia 2016/679 to administrator w określonych przypadkach konsultuje się z organem nadzorczym przed rozpoczęciem przetwarzania danych. Jest to następstwem spoczywających na nim – jako na podmiocie ustalającym cele i sposoby przetwarzania – obowiązków, w tym przypadku konieczności przeprowadzenia oceny skutków dla ochrony danych i zidentyfikowania oraz zminimalizowania ryzyka naruszenia praw lub wolności osób fizycznych. Konsultując się z organem nadzorczym administrator przedstawia mu m.in. obowiązki podmiotów przetwarzających (art. 36 ust. 3 lit. a rozporządzenia 2016/679). W niektórych przypadkach pisemne zalecenia będą zatem skierowane do podmiotu przetwarzającego (art. 36 ust. 2 rozporządzenia 2016/679), lecz będzie to nierozerwalnie związane z przetwarzaniem przez niego danych na zlecenie administratora w konkretnym stanie faktycznym, opisanym we wniosku złożonym przez administratora. Ponadto zauważyć należy, że przepisy rozporządzenia 2016/679 nie nakładają na podmiot przetwarzający obowiązku dokonania oceny skutków dla ochrony danych – a stanowi ona obligatoryjny element wniosku o przeprowadzenie uprzednich konsultacji (art. 36 ust. 3 lit. e rozporządzenia 2016/679), co również przesądza, że wnioskodawcą może być wyłącznie administrator.

Reasumując, w świetle przepisów rozporządzenia 2016/679 wyłącznie administrator może wystąpić do organu nadzorczego z wnioskiem o przeprowadzenie uprzednich konsultacji.

Uwzględniając powyższe, proponuję następujące brzmienie art. 57:

„Art. 57. 1. Administrator może wystąpić do Generalnego Inspektora/Prezesa Urzędu/ z wnioskiem o przeprowadzenie uprzednich konsultacji, o którym mowa w art. 36 rozporządzenia 2016/679.

2. Do wniosku stosuje się odpowiednio art. 63 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Jeżeli wniosek nie spełnia wymogów, określonych w art. 36 ust. 3 rozporządzenia 2016/679 oraz w art. 63 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, Generalny Inspektor/Prezes Urzędu/ informuje o nieudzieleniu konsultacji wskazując przyczyny jej nieudzielenia.".

Postępowanie kontrolne. Generalny Inspektor Ochrony Danych Osobowych podtrzymuje swoją propozycję dodania do **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** przepisu wyłączającego zastosowanie niektórych przepisów ustawy – Prawo przedsiębiorców. Propozycja przepisu brzmi następująco:

„Art. .... Do kontroli działalności gospodarczej przedsiębiorcy, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2018 r. poz. 646), z wyłączeniem art. 48, art. 54 i 55 tej ustawy, w przypadku istnienia uzasadnionego podejrzenia naruszenia przepisów rozporządzenia 2016/679.".

Zasadą będzie stosowanie przepisów art. 48 ustawy – Prawo przedsiębiorców, ponieważ informowanie z wyprzedzeniem o kontroli leży też w interesie organu, np. przygotowanie dokumentów, obecność osób uprawnionych do reprezentacji przedsiębiorcy w toku kontroli itp. Jednak w szczególnej sytuacji, tj. kiedy istnieje uzasadnione podejrzenie naruszenia przepisów rozporządzenia 2016/679, np. wyciek danych, kontrola bez wcześniejszego powiadomienia uniemożliwi przedsiębiorcy zatarcie lub usunięcie dowodów, które będą miały istotny wpływ na ustalenie stanu faktycznego, a następnie na wysokość zastosowanej wobec przedsiębiorcy kary finansowej.

Naruszenie przepisów rozporządzenie 2016/679, takie jak np. wyciek danych, może wystąpić wielokrotnie w ciągu roku. Nie jest możliwe przewidzenie, ile incydentów dotyczących naruszenia ochrony danych osobowych będzie miało miejsce u danego przedsiębiorcy w danym roku kalendarzowym. Ponadto w odniesieniu do jednego przedsiębiorcy może zostać złożonych wiele skarg o różnym zakresie przedmiotowym. Z dotychczasowej praktyki organu wynika, że takie naruszenie jest niezależne od wielkości przedsiębiorcy, a limit dni kontroli i brak możliwości jej wykonywania w tym samym czasie co inny organ kontroli (nawet z wykorzystaniem możliwości przeprowadzenia powtórnej kontroli – dodatkowe 7 dni) może uniemożliwić skontrolowanie przedsiębiorcy w danym roku kalendarzowym. Należy zatem podkreślić, że wyznaczenie limitu czasu trwania kontroli jest szczególnie nieuzasadnione w przypadku kontroli prowadzonych na skutek skarg oraz powzięcia informacji o naruszeniu ochrony danych (w szczególności podlegającemu zgłoszeniu Prezesowi Urzędu

na zasadach, o których mowa w art. 33 rozporządzenia 2016/679) skutkującego prawdopodobnym ryzykiem naruszenia praw i wolności osób fizycznych. Wprowadzenie limitu kontroli może ograniczyć możliwość realizacji uprawnień organu nadzorczego w przypadkach, gdy w danym roku kalendarzowym zostanie wyczerpany omawiany limit. Należy pamiętać również o tym, że prawo ochrony danych jest prawem podstawowym, a kontrole prowadzone przez organ w tym zakresie mają na celu ustalenie stanu faktycznego w zakresie przestrzegania przez podmiot kontrolowany przepisów o ochronie danych osobowych. Uniemożliwienie organowi wykonywania wyżej wymienionych zadań może wpłynąć również na sytuację osób, które dochodzą swoich praw. Ponadto, co jest niezwykle istotne i powinno być brane pod uwagę przez projektodawcę przy tak wysokich karach, jakie będzie mógł stosować Prezes Urzędu na podstawie przepisów rozporządzenia 2016/679, konieczne będzie staranne ustalenie stanu faktycznego przez organ, a to będzie wiązało się z koniecznością prowadzenia kontroli bez ograniczeń czasowych.

Dotychczasowe doświadczenie Generalnego Inspektora Ochrony Danych Osobowych pozwala stwierdzić, że bezpieczeństwo danych osobowych nie ma żadnej korelacji z wielkością przedsiębiorcy (np. mikroprzedsiębiorca może mieć większą ilość klientów, tj. osób fizycznych, i tym samym większą bazę danych albo przetwarzać dane osobowe w szerszym zakresie, np. dane szczególnie chronione, aniżeli np. średni przedsiębiorca). Nie jest więc zasadne limitowanie czasu kontroli w zależności od wielkości przedsiębiorcy i osiąganych przez niego dochodów, ponieważ nie ma to przełożenia na zakres i cel kontroli.

Podkreślić przy tym trzeba, że wielokrotne naruszanie przepisów rozporządzenia 2016/679 w ciągu roku przez tego samego przedsiębiorcę ma przełożenie na prawa i wolności osób, których dane dotyczą i w sytuacji uzasadnionego podejrzenia naruszenia przepisów rozporządzenia 2016/679 przez takiego przedsiębiorcę, organ kontroli nie powinien mieć ograniczeń wynikających z art. 48, 54 i 55 ustawy – Prawo przedsiębiorców.

Czas trwania kontroli (art. 89 projektu ustawy). Generalny Inspektor Ochrony Danych Osobowych podtrzymuje uwagę dotyczącą czasu trwania kontroli, o której mowa w art. 89 ust. 1 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**. Wskazany przepis przewiduje konieczność zachowania trzydziestodniowego terminu na zakończenie kontroli. Przypomnieć należy, że ze względu na specyfikę kontroli, często bardzo szeroki zakres przedmiotu kontroli, wymóg dotyczący terminu powinien być mniej restrykcyjny. Proponuję przeredagowanie tego przepisu poprzez użycie sformułowania „postępowanie kontrolne nie powinno trwać dłużej niż dwa miesiące" lub termin powinien dotyczyć zakończenia czynności kontrolnych, a nie kontroli. Należy przewidzieć sytuacje,

w których będzie potrzeba prowadzenia czynności tak długo, jak będzie to konieczne do pełnego wyjaśnienia stanu faktycznego (np. w przypadku bardzo zaawansowanych technologii służących do przetwarzania danych osobowych, prowadzenia kontroli międzynarodowych), a zachowanie krótkiego terminu (w którym powinny zostać zakończone zarówno czynności kontrolne, jak i sporządzony protokół kontroli dokumentujący przebieg czynności kontrolnych) nie będzie możliwe. Ponadto – co jest szczególnie istotne – sposób organizacji pracy kontrolujących, który nie zawsze będzie zależny od Prezesa Urzędu oraz specyfika prowadzonych kontroli, może mieć wpływ na dochowanie terminu zakończenia kontroli, np. konieczność przeprowadzenia od razu czynności kontrolnych przez tych samych kontrolujących w kolejnym podmiocie, co uniemożliwi sporządzenie protokołu zaraz po kontroli. Jednocześnie Generalny Inspektor Ochrony Danych Osobowych zwraca uwagę, że obowiązujące przepisy regulujące postępowania kontrolne prowadzone przez inne organy nie przewidują takiego czasowego ograniczenia – dotyczą jedynie czasu trwania kontroli u przedsiębiorcy, a nie całej kontroli. Konsekwencją przyjętego rozwiązania będzie konieczność prowadzenia u danego przedsiębiorcy kilku następujących po sobie kontroli, których czas trwania pozwoli na pełne wyjaśnienie sprawy. W rzeczywistości może oznaczać to, że czas trwania czynności kontrolnych będzie znacznie wydłużony. Najlepszym rozwiązaniem byłoby wskazanie, że sporządzenie protokołu kontroli powinno nastąpić niezwłocznie po zakończeniu czynności kontrolnych, zamiast rygorystycznego wskazania terminu zakończenia czynności kontrolnych łącznie ze sporządzeniem i podpisaniem protokołu przez kontrolowanego. Należy podkreślić, że Prezes Urzędu będzie prowadził nie tylko kontrole przedsiębiorców, ale także innych podmiotów, m.in. organów publicznych. Ograniczenie terminu nie powinno zatem dotyczyć tych podmiotów, które nie maja statusu przedsiębiorcy.

Przepisy dotyczące odpowiedzialności cywilnej (rozdział 10).

Generalny Inspektor Ochrony Danych Osobowych wielokrotnie zgłaszał wątpliwości co do przedstawionej przez ustawodawcę wizji unormowań regulujących postępowanie cywilne dotyczące naruszeń przepisów o ochronie danych osobowych. Zamiarem prawodawcy unijnego było zapewnienie osobom, których prawo do ochrony danych osobowych zostało naruszone lub zagrożone, możliwości obrony ich praw i wolności zarówno przed niezależnym organem nadzorczym, jak i przed sądem powszechnym (art. 79 ust. 1 rozporządzenia 2016/679). Tymczasem ustawodawca tak ukształtował przepisy rozdziału 10 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**, by uniemożliwić osobom, których prawo do ochrony danych osobowych zostało naruszone lub zagrożone, takie dwutorowe dochodzenie

ich praw. W ocenie GIODO przyjęte w rozdziale 10 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** rozwiązania budzą uzasadnione wątpliwości co do ich zgodności z rozporządzeniem 2016/679.

Nie można zgodzić się z art. 97 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**, który wprowadza, nieznane dotychczas polskiemu ustawodawstwu, związanie niezawisłego sądu decyzją organu administracji publicznej, jakim jest Prezes Urzędu Ochrony Danych Osobowych. Jedynym znanym w prawie polskim przypadkiem związania przy orzekaniu sądu cywilnego rozstrzygnięciem innego podmiotu jest prejudycjalność wyroków sądów karnych. Jednakże sytuacja taka dotyczy jedynie faktu popełnienia przestępstwa (który to fakt zostaje stwierdzony prawomocnym wyrokiem sądu karnego) oraz oznacza związanie jednego niezawisłego sądu wyrokiem innego niezawisłego sądu. Nie można takiej sytuacji – w świetle art. 45 ust. 1 Konstytucji Rzeczypospolitej Polskiej – odnosić do relacji, jaka zachodzi między decyzją administracyjną organu administracji publicznej a wyrokowaniem przez sąd. Tym samym art. 97 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** budzi wątpliwości również co do zgodności z Konstytucją Rzeczypospolitej Polskiej. Jednocześnie, skoro ustawodawca, co jest wątpliwe w świetle postanowień rozporządzenia 2016/679, chce zawieszać jedno z postępowań dotyczących naruszeń przepisów o ochronie danych osobowych, to zawieszenie to powinno dotyczyć postępowania prowadzonego przed Prezesem Urzędu Ochrony Danych Osobowych, nie postępowania przed niezawisłym sądem. Zaproponowane brzmienie art. 95 powinno zostać przeredagowane w ww. zakresie. Zmiana brzmienia art. 95 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** w ten sposób, że zawieszane byłoby postępowanie przed Prezesem Urzędu Ochrony Danych Osobowych, a nie przed sądem, spowodowałaby, że bezprzedmiotowy będzie art. 96 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** i należy go usunąć.

Generalny Inspektor Ochrony Danych Osobowych podtrzymuje swoje uwagi dotyczące konieczności wprowadzenia do **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** następującego przepisu:

„Art..... 1. Każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, może żądać nakazania przez sąd przywrócenia stanu zgodnego z prawem.

2. Wystąpienie z roszczeniem, o którym mowa w ust. 1, nie wyłącza możliwości wystąpienia, w związku z naruszeniem przepisów o ochronie danych osobowych, z innymi roszczeniami na zasadach ogólnych.".

Administracyjne kary pieniężne (art. 101 i 102). Zgodnie z **ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych**, podmioty publiczne, o których mowa w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych oraz Narodowy Bank Polski za naruszenie przepisów o ochronie danych osobowych będą zagrożone sankcją czterystukrotnie niższą od przewidzianej w rozporządzeniu 2016/679. Przewidziana dla podmiotów publicznych administracyjna kara pieniężna 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 takiej wysokości nie spełnią ani funkcji represyjnej, ani funkcji prewencyjnej. Posługując się językiem rozporządzenia 2016/679, kara administracyjna w wysokości do 100 tys. zł nie będzie „skuteczna, proporcjonalna i odstraszająca". W ocenie Generalnego Inspektora Ochrony Danych Osobowych 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.

Ponadto, obniżenie kar w stosunku do sektora publicznego może powodować obniżenie poziomu ochrony danych osobowych przez te jednostki, które zamiast dążyć do zachowania pełnej zgodności z rozporządzeniem 2016/679, będą liczyły się z ewentualną karą pieniężną, która zostanie pokryta ze środków publicznych. Natomiast podmiot prywatny, który za ewentualne naruszenie ochrony danych zapłaci swoimi środkami pieniężnymi, nie będzie mógł pozwolić sobie na niedociągnięcia w zakresie zgodności z rozporządzeniem 2016/679. Należy również pamiętać o tym, z jak szerokiego katalogu danych o osobach korzystają podmioty publiczne.

W ocenie GIODO dane obywateli powinny być traktowane w równy sposób, niezależnie od tego, czy przetwarza je administrator podmiotu publicznego czy prywatnego. Ten problem można zobrazować przykładem: Jaka jest 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.

Brak równości podmiotów publicznych wobec stosowania do nich kar pieniężnych. Generalny Inspektor Ochrony Danych Osobowych podtrzymuje uwagę dotyczącą katalogu podmiotów publicznych określonych w art. 102 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**. Rozważając kwestię wysokości kar należy przede wszystkim zwrócić uwagę na kwestię równości podmiotów. **Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** w art. 102 ust. 2 zakłada obniżenie kary za naruszenie przepisów rozporządzenia 2016/679 przez państwowe i samorządowe instytucji kultury do 10 tys zł. Projektodawca w uzasadnieniu projektu ustawy wskazywał, że na specjalne traktowanie tych instytucji wpływa ich niski budżet, a zakres przetwarzanych danych osobowych nie powoduje znaczącego zagrożenia dla prywatności użytkowników oraz powoływał się na fakt, że kultura jest traktowana w wielu regulacjach w sposób szczególny, np. do działalności kulturalnej w pewnym zakresie nie stosuje się w ogóle Prawa zamówień publicznych. W ocenie Generalnego Inspektora Ochrony Danych Osobowych porównywanie regulacji dotyczącej prawa ochrony danych, czyli jednego z praw podstawowych, do regulacji dotyczącej zasad i trybu udzielania zamówień publicznych, nie wpisuje się w założenia reformy mającej na celu wzmocnienie praw osób fizycznych. Nie można również zgodzić się z poglądem, że zakres danych przetwarzanych przez instytucje kultury nie powoduje zagrożenia dla prywatności. Ustawodawca zdaje się zapominać, że muzea mogą mieć zainstalowany monitoring, który pozwala na zidentyfikowanie osoby, a na podstawie karty bibliotecznej można poznać zainteresowania osoby korzystającej z usług biblioteki w zakresie dotyczącym poglądów politycznych, wyznania lub przekonań. Zgodnie z rozporządzeniem 2016/679 takie dane należą do szczególnej kategorii danych, co znaczy, że są szczególnie wrażliwe w świetle podstawowych praw i wolności, i wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności (motyw 51 rozporządzenia). W ocenie Generalnego Inspektora Ochrony Danych Osobowych tak znaczące obniżenie administracyjnej kary pieniężnej, która może zostać nałożona na te instytucje, nie jest uzasadnione, szczególnie z punktu widzenia osób, których dane dotyczą. Nie należy również zapominać, że jednym z celów rozporządzenia 2016/679 jest zapewnienie równorzędnych uprawnień w zakresie monitorowania i egzekwowania przepisów

o ochronie danych osobowych oraz równorzędnych kar za naruszenia tych przepisów w państwach członkowskich (motyw 11 rozporządzenia).

Brak jednolitości przepisów o monitoringu wizyjnym (art. 111, 114, 122, 123, 154, 155). Wątpliwym jest przyjmowanie przepisów regulujących monitoring wizyjny w różnych obszarach, które nie są ze sobą spójne. Propozycje ujęte w art. 111 i 154 dot. możliwości monitorowania pomieszczeń zasadniczo wyłączonych spod takiej formy nadzoru pozostaje w sprzeczności z przepisami art. 114, 122, 123 i 155. Generalny Inspektor Ochrony Danych Osobowych postuluje wyłączenie możliwości monitorowania pomieszczeń, w których osoby obserwowane mają uzasadnione oczekiwanie ochrony prywatności i intymności. W szczególności dotyczy to sytuacji, gdy możliwy jest nadzór uczniów przez opiekunów w placówce oświatowej i pracowników przez osoby nadzorujące w zakładzie pracy.

Uwagę Generalnego Inspektora zwracają także przepisy zapobiegające niszczeniu nagrań, gdy zastosowanie znajdują przepisy odrębne. Postanowienia te nie zostały uzasadnione, tym samym nie jest jasnym, w jakich sytuacjach i jak długo wymagane będzie przechowywanie nagrań. W przypadku zakładów pracy nie powinno to obejmować przepisów dot. postępowań dyscyplinarnych, jako że stosowanie monitoringu wizyjnego ma być dopuszczalne w innych niż ocena pracownika celach.

Podział funkcji administratora w zależności od postaci danych przetwarzanych przez prokuraturę (art. 149). Za wątpliwe rozwiązanie uznać należy podział kompetencji administratora pomiędzy Prokuraturę Krajową (dane w ogólnokrajowych systemach teleinformatycznych powszechnych jednostek organizacyjnych prokuratury) a powszechne jednostki organizacyjne prokuratury (dane przetwarzane w ramach realizowanych zadań z wyłączeniem danych w w/w systemach). W sytuacji takiej zastosowanie mogłyby mieć przepisy o właściwości organów prokuratury ujęte w ustawie.

Na szczególną uwagę zasługuje wyłączenie stosowania art. 12-16 i 18-22 rozporządzenia 2016/679 w postępowaniach lub systemach teleinformatycznych w ramach realizacji zadań prokuratury w zakresie ścigania przestępstw. Propozycja ta nie została w żaden sposób uzasadniona oraz może nie spełniać wymogów ujętych w art. 23 rozporządzenia 2016/679.

Stosowanie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (art. 160 ust. 2). Poważne wątpliwości Generalnego Inspektora Ochrony Danych Osobowych

budzi zaproponowane brzmienie art. 160 ust. 2 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**. Przedmiotowy przepis interpretowany literalnie skutkowałby zachowaniem mocy obowiązującej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i to przez nieokreślony czas (terminu zakończenia prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych postępowań nie da się określić). Co więcej – w okresie między 25 maja 2018 r. (gdy zacznie być bezpośrednio stosowane w prawie polskim rozporządzenie 2016/679) a datą zakończenia prowadzenia przez Prezesa Urzędu Ochrony Danych Osobowych (zgodnie z art. 160 ust. 1 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych**) ostatniego „starego" (czyli wszczętego i niezakończonego przez Generalnego Inspektora Ochrony Danych Osobowych do dnia 25 maja 2018 r.) postępowania, istniałyby dwa prawa materialne: ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, w oparciu o przepisy której miałyby być oceniane stany faktyczne w postępowaniach „starych", i rozporządzenie 2016/679 dla stanów faktycznych w postępowaniach wszczętych od dnia 25 maja 2018 r.

W opinii GIODO rozwiązanie takie nie może być zaakceptowane w świetle wyrażonej w art. 288 zdanie trzecie Traktatu o funkcjonowaniu Unii Europejskiej zasady bezpośredniego stosowania w państwach członkowskich przepisów rozporządzeń unijnych. Nie można również pominąć konsekwencji wynikających z art. 91 ust. 3 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym: „Jeżeli wynika to z ratyfikowanej przez Rzeczpospolitą Polską umowy konstytuującej organizację międzynarodową, prawo przez nią stanowione jest stosowane bezpośrednio, mając pierwszeństwo w przypadku kolizji z ustawami". Biorąc pod uwagę, iż rozporządzenie 2016/679 spełnia wszystkie wymagania wskazane w art. 91 ust. 3 Konstytucji Rzeczypospolitej Polskiej, także w świetle prawa polskiego po dniu 24 maja 2018 r. nie jest dopuszczalne stosowanie przepisów aktualnie obowiązującej ustawy o ochronie danych osobowych w takim zakresie, w jakim do danego stanu faktycznego znajdują zastosowanie przepisy rozporządzenia 2016/679.

Biorąc po uwagę powyższe przepis art. 160 ust. 2 **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** nie może zyskać akceptacji.

Uwagi o charakterze redakcyjno – legislacyjnym. Generalny Inspektor zwraca uwagę na kilka koniecznych zmian, które należy wprowadzić do projektu:

1. **uwaga do art. 11**

W dalszym ciągu pozostaje aktualna – zgłaszana w czasie uzgodnień – uwaga GIODO co do zasadności i celowości upubliczniania imienia i nazwiska inspektora ochrony danych. Przypomnieć należy, że art. 37 ust. 7 rozporządzenia 2016/679 nakłada na administratora lub podmiot przetwarzający obowiązek publikowania jedynie danych kontaktowych inspektora ochrony danych.

Art. 11 powinien otrzymać następujące brzmienie: „Art. 11. Podmiot, który wyznaczył inspektora, udostępnia dane kontaktowe inspektora, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.".

2. **uwaga do art. 25 ust. 1 pkt 2**

Obecnie przepis brzmi: „2) wglądu do dokumentów i informacji mających bezpośredni związek z działalnością objętą certyfikacją".

Proponuje się zastąpić sformułowanie „działalnością objęta certyfikacją" na „przedmiotem udzielonej certyfikacji". W przypadku certyfikacji produktu, sam produkt trudno nazwać działalnością objętą certyfikatem.

3. **uwaga do art. 158 ust. 1-2 oraz 4**

Obecnie przepis brzmi: ,,1. Osoba pełniąca w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, o którym mowa w ustawie uchylanej w art. 175, staje się, inspektorem ochrony danych i pełni swoją funkcje do dnia 1 września 2018 r., chyba, że przed tym dniem administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na inspektora ochrony danych, w sposób określony w art. 10 ust. 1.

2. Osoba, która stała się, inspektorem ochrony danych, na podstawie ust. 1, pełni swoją funkcję także po dniu 1 września 2018 r., jeżeli do tego dnia administrator zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o jej wyznaczeniu w sposób określony w art. 10 ust. 1."

Proponuję zmianę na : ,,1. Osoba pełniąca w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, o którym mowa w ustawie uchylanej w art. 175, staje się, inspektorem ochrony danych i pełni swoją funkcje do dnia 1 września 2018 r., chyba, że przed tym dniem administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na inspektora ochrony danych, w sposób określony w art. 10 ust. 1-6.

2. Osoba, która stała się, inspektorem ochrony danych, na podstawie ust. 1, pełni swoją funkcję także po dniu 1 września 2018 r., jeżeli do tego dnia administrator zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o jej wyznaczeniu w sposób określony w art. 10 ust. 1-6.''.

Obecnie przepis brzmi: „4. Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał administratora bezpieczeństwa informacji, o którym mowa w ustawie uchylanej w art. 175, jest obowiązany do wyznaczenia inspektora ochrony danych na podstawie art. 37 rozporządzenia 2016/679, i zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu, w terminie do dnia 31 lipca 2018 r.".

Proponuję zmiana na : „4. Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał administratora bezpieczeństwa informacji, o którym mowa w ustawie uchylanej w art. 175, a jest zobowiązany do wyznaczenia inspektora ochrony danych na podstawie art. 37 rozporządzenia 2016/679, wyznacza inspektora ochrony danych i zawiadamia Prezesa Urzędu o jego wyznaczeniu, w terminie do dnia 31 lipca 2018 r.".

Zwracam się z uprzejmą prośbą o przekazanie niniejszego pisma organom Senatu oraz senatorom na Senat RP.

Z wyrazami szacunku,

z up. Generalnego
Inspektora Ochrony Danych Osobowych
Z-ca Generalnego
Inspektora Ochrony Danych Osobowych
Mirosław Sanek

Otrzymują:

1. Pan Jacek Czaputowicz – Minister Spraw Zagranicznych
2. Pan Marek Zagórski – Sekretarz Stanu w Ministerstwie Cyfryzacji
3. Pan Adam Bodnar – Rzecznik Praw Obywatelskich