

**Uwagi Generalnego Inspektora Ochrony Danych Osobowych**  
**do projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**

**1. Założenia projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**

Na wstępie należy zauważyć, że przepis art. 1 projektowanej ustawy ma informować o tym, czego dotyczy ustawa wprowadzająca. „Stosowanie tej instytucji ma służyć zwiększaniu czytelności systemu prawnego i czytelności danej ustawy, gdyż dzięki przeniesieniu przepisów zmieniających, uchylających, epizodycznych, przejściowych, dostosowujących i końcowych do osobnej ustawy, w ustawie "głównej" pozostawia się tylko przepisy merytoryczne.” (Wierczyński Grzegorz, Komentarz do rozporządzenia w sprawie "Zasad techniki prawodawczej", [w:] Redagowanie i ogłaszanie aktów normatywnych. Komentarz, wyd. II). Również Trybunał Konstytucyjny odniósł się do szczególnego charakteru ustawy wprowadzającej. W wyroku z dnia 28 lutego 2008 r., K 43/07, Trybunał stwierdził, że "najważniejszym celem ustawy wprowadzającej, poza "odciążeniem" ustawy głównej, by była ona bardziej przejrzysta, jest uchylenie niektórych dotychczasowych przepisów, uregulowanie spraw będących w toku, przekazanie kompetencji, utworzenie instytucji czy uporządkowanie pewnych kwestii zaniedbanych wcześniej przez ustawodawcę, aby stworzyć podstawy do wejścia w życie przepisów ustawy wprowadzanej". W sprawie K 43/07 Trybunał wskazał, że analiza i ocena rozwiązań zawartych w przepisach wprowadzających musi być zatem dokonywana z uwzględnieniem szczególnego charakteru ustawy wprowadzającej.

Biorąc pod uwagę powyższe wydaje się, że w przedstawionych przez Ministra Cyfryzacji przepisach powinny znaleźć się tylko i wyłącznie regulacje, które mają na celu przygotowanie krajowego porządku prawnego do stosowania rozporządzenia 2016/679 oraz nowej ustawy o ochronie danych osobowych.

W tym kontekście wątpliwości budzi zakres zmian zaproponowanych w ustawie z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (Dz. U. z 2017 r. poz. 1007), ustawie z dnia 21 marca o drogach publicznych (Dz. U. z 2016 r. poz. 1440 z późn. zm.), ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2017 r. poz. 880 i 1089) oraz zmiany

proponowane w dużej części ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2016 r. poz. 1068 oraz z 2017 r. poz. 60 i 885).

Generalny Inspektor Ochrony Danych Osobowych zauważa, że krajowa reforma ochrony danych osobowych została wykorzystana przez projektodawcę jako pretekst dla wprowadzenia w przepisach wprowadzających zmian w dotychczas obowiązujących ustawach, które nie pozostają w związku z przygotowaniem polskiego systemu prawnego do stosowania rozporządzenia 2016/679. Niektóre zmiany zaproponowane w ww. ustawach nie pozostają w związku z tym procesem oraz zasadniczo i niekorzystnie, z punktu widzenia ochrony danych osobowych, modyfikują istniejące rozwiązania, które zostały wypracowane często w toku wieloletnich uzgodnień z organem do spraw ochrony danych osobowych i których końcowym efektem było zapewnienie właściwej ochrony osób, których dane dotyczą. Niepokojącą i nieuzasadnioną z punktu widzenia stosowania rozporządzenia 2016/679 ingerencją w obecny poziom ochrony danych obywateli są zmiany w ustawie o statystyce publicznej. Przypomnieć należy, iż celem rozporządzenia 2016/679 jest podwyższenie poziomu ochrony danych osobowych w Unii Europejskiej. Wszelkie zmiany krajowych przepisów sektorowych obniżające ten poziom nie mogą być uznane za zgodne z kierunkiem rozwiązań przyjętych w rozporządzeniu 2016/679.

## **2. Wyłączenie w przepisach krajowych przepisów rozporządzenia 2016/679, normujących prawa osób, których dane dotyczą**

Zdecydowany sprzeciw Generalnego Inspektora Ochrony Danych Osobowych budzą przepisy dotyczące wyłączenia stosowania art. 5, 12 - 22, 34 rozporządzenia 2016/679 do procesów przetwarzania danych osobowych, o których mowa w licznych ustawach zmienianych w przedmiotowym projekcie.

Generalny Inspektor przypomina, że art. 23 rozporządzenia 2016/679 dotyczy dopuszczalności ograniczenia w prawie państwa członkowskiego zakresu obowiązków i praw przewidzianych w art. 12 – 22 i w art. 34, a także w art. 5 oraz wskazuje zasady i warunki takiego ograniczenia. Przepisy prawa krajowego przewidujące ograniczenia w tym zakresie muszą jednocześnie odpowiadać prawom i obowiązkom przewidzianym w art. 12 – 22, nie mogą naruszać istoty podstawowych praw i wolności oraz muszą stanowić – w demokratycznym społeczeństwie – środek niezbędny i proporcjonalny, służący określonym, wymienionym enumeratywnie w art. 23 ust. 1 wartościom, spełniając obligatoryjnie szczegółowe warunki określone w art. 23 ust. 2 rozporządzenia 2016/679.

Istotą uprawnienia z art. 23 rozporządzenia 2016/679 nie jest wyłączenie stosowania art. 5, 12-22, 34 w taki sposób, jakiego dokonał Minister Cyfryzacji w swoim projekcie ustawy. Projektodawca w większości przypadków w przepisach projektu ustawy - Przepisy wprowadzające używa sformułowania „nie stosuje się” bez wskazania uzasadnienia takiego działania oraz dokonania wnikliwej analizy, które konkretne przypadki, przy zachowaniu określonych w rozporządzeniu 2016/679 zasad, mogą podlegać ograniczeniom. na co wskazuje również tytuł art. 23 rozporządzenia 2016/679 – „ograniczenia”.

Zaproponowane w przepisach projektu ustawy zmiany będą w konsekwencji powodowały nieprawidłowe stosowanie przepisów rozporządzenia 2016/679 przez wiele podmiotów, zarówno z sektora publicznego, jak i prywatnego. Przeprowadzając reformę krajowych przepisów dotyczących ochrony danych projektodawca powinien zaproponować takie przepisy, które będą zapobiegały naruszeniu praw i wolności osób, których dane dotyczą, a nie, jak pokazuje to niniejszy projekt, doprowadzenie do pozbawienia podmiotów danych tychże praw. Generalny Inspektor zdecydowanie sprzeciwia się takiej praktyce.

Generalny Inspektor zauważa również, że projektodawca wyłączając obowiązki i prawa przewidziane w art. 12 – 22 i w art. 34, a także w art. 5 rozporządzenia 2016/679 opiera się przede wszystkim na przesłance określającej „inne ważne cele leżące w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważny interes gospodarczy lub finansowy Unii lub państwa członkowskiego, w tym kwestii pieniężnych, budżetowych i podatkowych, zdrowia publicznego i zabezpieczenia społecznego” (art. 23 ust. 1 lit e rozporządzenia 2016/679). Takie uzasadnienie jest niewystarczające oraz zbyt ogólne. Jednocześnie nie jest dostatecznie wyjaśnione na podstawie jakich analiz, w szczególności ekonomicznych, została oparta decyzja o wyłączeniu stosowania rozporządzenia 2016/679. W tym miejscu warto przypomnieć stanowisko prezentowane w orzecznictwie NSA wskazujące na to, że względy natury organizacyjno-finansowej nie powinny być traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych. Powyższe stanowisko w pełni zachowuje aktualność, również na gruncie rozporządzenia 2016/679.

Analiza zaproponowanych przez Ministra Cyfryzacji wyłączeń sprowadza się do sformułowania tezy o braku zasadności ich zastosowania przez Projektodawcę wyłączeń – a w niektórych przypadkach ograniczeń – obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 RODO zastosowanych przez Projektodawcę. Projektodawca musi dokonać w wielu przypadkach ponownej analizy stosowanych wyłączeń przy uwzględnieniu Rozdziału IX

rozporządzenia 2016/679 zatytułowanego „Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem”, zbadał oraz wykazał ich rzeczywistą niezbędność.

Generalny Inspektor odnosi się w swoich uwagach do art. 21 projektu, i uwagi tr pozostają aktualne również do innych ustaw zmienianych projektem.

Podnieść należy, że rozporządzenie 2016/679 kładzie nacisk na **uprawnienia osób, których dane dotyczą**, wskazując w motywie 11, że aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić i doprecyzować prawa osób, których dane dotyczą, oraz obowiązki podmiotów przetwarzających dane osobowe i decydujących o przetwarzaniu, jak również zapewnić równorzędne uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych oraz równorzędne kary za naruszenia tych przepisów w państwach członkowskich. Należy zatem ze szczególną ostrożnością pochylić się nad kwestią proponowanych ograniczeń i wyłączeń obowiązków administratorów i podmiotów przetwarzających, jakie mają te podmioty w stosunku do osób, których dane dotyczą.

Prawodawca unijny umożliwi państwom członkowskim ograniczenie zastosowania art. 12 – 22, art. 34 oraz art. 5 rozporządzenia 2016/679, jedynie w przypadkach opisanych w art. 23 ust. 1 rozporządzenia, przy jednoczesnym zachowaniu wymogów określonych w art. 23 ust. 2. Brak jest zatem zupełnej dowolności w zakresie możliwości wyłączenia zastosowania ww. przepisów przez ustawodawcę krajowego.

**3. Wyłączenie zasady rozliczalności.** Niepokojące są proponowane w części przepisów wyłączenia zasady rozliczalności, która jest fundamentalna dla unijnej reformy ochrony danych. Należy przypomnieć, że została ona podniesiona z poziomu wykazywania zgodności technicznej z przetwarzaniem danych (np. zgodnie z art. 36 obowiązującej jeszcze ustawy o ochronie danych osobowych) do obowiązku wykazania wypełnienia wszystkich zasad i obowiązków wobec osób, których dane dotyczą. Zgodnie z przepisem art. 5 ust. 2 rozporządzenia 2016/679 administrator musi być w stanie wykazać, że przetwarzanie danych, w tym ich udostępnienie innym podmiotom jest adekwatne, stosowne oraz ograniczone do tego co niezbędne dla celów, w których są przetwarzane. Projektodawca powinien każdorazowo wyjaśnić i wyczerpująco uzasadnić te kwestie, aby uniknąć nieporozumień co do obowiązywania unijnej reformy w określonych sektorach regulowanych zmienianymi przepisami.

Niestety projektodawca proponując wyłączenie czy ograniczenie uprawnień podmiotów danych, nie przedstawił w oparciu o katalog okoliczności uprawniających do zastosowania ograniczeń wymieniony w art. 23 ust. 1 rozporządzenia 2016/679, szczegółowych przyczyn

zastosowanych wyłączeń. Nie wyważył również interesów podmiotu danych oraz administratora i podmiotu przetwarzającego i nie wykazał sprzeczności tych interesów, uzasadniających zastosowane wyłączenie. Projektodawca nie wykazał również dlaczego ograniczenie uprawnień podmiotu danych jest niezbędne oraz pominął konieczność jednoczesnego wypełnienia warunków określonych w art. 23 ust. 2 rozporządzenia 2016/679.

Osoby, których dane dotyczą nie mogą zostać pozbawione praw przysługujących im na gruncie przepisów rozporządzenia 2016/679 w sposób niezgodny z przepisami rozporządzenia. Zaproponowane wyłączenia są niedopuszczalne i stoją w sprzeczności z zasadą bezpośredniego stosowania prawa wspólnotowego oraz zasadą prymatu prawa wspólnotowego. Stanowisko to znajduje potwierdzenie w orzecznictwie Trybunału Sprawiedliwości w sprawie 6/64 Flaminio Costa przeciwko E.N.E.L., w którym Trybunał wskazał, że prawo wywodzące się z Traktatu nie może być podważone przez ustawy krajowe.. Państwo członkowskie nie może powołać się na żadne normy swojego porządku prawnego, które byłyby wyłączone spod działania zasady prymatu prawa wspólnotowego. Natomiast w orzeczeniu Trybunału Sprawiedliwości w sprawie Van Gend i Loos 26/62 zwrócono uwagę na zasadę bezpośredniej skuteczności prawa wspólnotowego. Wyrok ten wpłynął na rozszerzenie ochrony praw osób, które zyskały możliwość powołania się na normy prawa wspólnotowego przed sądami krajowymi.

**4. Retencja danych.** Niedopuszczalne są również przedstawione przez Ministra Cyfryzacji propozycje okresu retencji danych osobowych przez podmiot uprawniony do ich przetwarzania. W większości ustaw, których zmianę zakłada projekt ustawy - Przepisy wprowadzające, okres przechowywania danych został ujęty w sposób lakoniczny i nieprecyzyjny, np. „termin ten ustala administrator mając na uwadze cele przetwarzania” lub mając na uwadze „przepisy odrębne dotyczące terminów”. Takie nieprecyzyjne określenie okresu przechowywania danych osobowych może prowadzić do przechowywania danych zbędnych do realizacji celu przez zbyt długi okres i tym samym prowadzić do naruszenia zasady ograniczenia przechowywania, określonej w art. 5 ust. 1 pkt e rozporządzenia 2016/679. Mając na uwadze motyw 39 rozporządzenia 2016/679, który wskazuje, że aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien zapewnić ograniczenia okresu przechowywania danych do ścisłego minimum, czyli ustalić termin ich usuwania lub okresowego przeglądu, koniecznym jest uregulowanie w konkretnych przepisach minimalnego, ale też odpowiedniego czasu przechowywania danych przez podmiot je przetwarzający.

**5. Pozyskiwanie danych.** W projektowanej ustawie brak jest rozwiązań w zakresie bezwioskowego pozyskiwania danych osobowych, np. za pomocą urządzeń teletransmisji danych, bez konieczności składania pisemnego wniosku. Taka forma dostępu do danych wiąże się np. z ryzykiem nadmiarowego udostępnienia danych (łączenie, kopie zbiorów), bowiem administrator danych traci możliwość weryfikacji, czy udostępnienie danych w każdym konkretnym przypadku można uznać za zgodne z prawem. Z przepisów prawa powinien jasno wynikać zakres, cel oraz zasady udostępniania danych, a podstawę takiego udostępnienia powinien stanowić wyłącznie wniosek. W tym kontekście na uwagę zasługuje w szczególności motyw 31 rozporządzenia 2016/679, zgodnie z którym żądanie ujawnienia danych osobowych, z którym występują organy publiczne powinno mieć zawsze formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych.

**6. Wskazywanie administratora w przepisach prawa.** Generalny Inspektor zwraca ponadto uwagę, że większość zmian polega jedynie na określaniu wprost w projektowanych przepisach statusu administratora poprzez wskazywanie podmiotu, który pełni rolę administratora w odniesieniu do konkretnych kategorii danych. Jednocześnie w przepisach zastosowano niezgodne z przepisami rozporządzenia 2016/679 określenia, jak: „administrator danych”, „administrator danych osobowych” czy „administrator danych i informacji”. Zazwyczaj ten zabieg jest podyktowany zakresem ustawowo uregulowanych kompetencji konkretnych podmiotów i wykonywanych przez nie zadań. Zwrócić uwagę należy, że niezwykle istotne jest zidentyfikowanie wszystkich kompetencji i obowiązków oraz wszelkich celów wynikających z konkretnych ustaw. Takie sztywne nadanie w ustawie statusu, nazwanie administratora, może rodzić w praktyce wątpliwości i spory co do kwestii jakiemu podmiotowi w konkretnej sytuacji należy przyznać ten status, np. w sytuacji rozbieżności w przepisach, w sytuacji zmiany kompetencji podmiotów, lub też tworzenia nowych organów lub podmiotów o podobnych kompetencjach. Biorąc pod uwagę definicję wynikającą z art. 4 pkt 7 rozporządzenia 2016/679, określenie „administrator” oznacza tego kto – będąc osobą fizyczną lub prawną, organem publicznym, jednostką lub innym podmiotem – samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczenia. Nie jest zatem konieczne, na gruncie rozporządzenia 2016/679, wyraźne wskazanie/ sprecyzowanie administratora lecz wyznaczenie jakie cele i sposoby przetwarzania danych będzie on realizował.

**7. Regulacje dotyczące pozyskiwania numeru PESEL.** Zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych budzą także zaproponowane regulacje dotyczące jawności numeru PESEL oraz skala pozyskiwania i wykorzystywania tej danej osobowej w kolejnych zbiorach czy rejestrach publicznych. Należy wskazać, że udostępnianie numeru PESEL, może prowadzić do nadmiernej i nieproporcjonalnej ingerencji w prawa osób, których dane znajdują się w różnych zbiorach danych osobowych. W świetle rozporządzenia 2016/679 identyfikator osoby musi być poddany szczególnej ochronie, w związku z czym należy stworzyć szczególne gwarancje wynikające z przepisów prawa, mając na względzie konieczność ich dostosowania do ww. rozporządzenia. Projektodawca tworząc nowe rozwiązania musi respektować zasady przetwarzania danych określone w rozporządzeniu 2016/679: ograniczenia celu (art. 5 ust. 1 pkt b) oraz minimalizacji danych osobowych (art. 5 ust. 1pkt c). Na projektodawcy ciąży odpowiedzialność za ewentualne negatywne konsekwencje proponowanych unormowań, w tym również związane z możliwością naruszenia konstytucyjnie gwarantowanych praw i wolności człowieka i obywatela (m.in. prawa do ochrony danych osobowych – art. 51 Konstytucji RP).

Mając na uwadze powyższe Generalny Inspektor sugeruje by w trakcie dokonywania zmian obowiązujących w polskim ustawodawstwie regulacji prawnych, czy też w związku z wprowadzaniem nowych rozwiązań – mających na celu sprostanie wymogom rozporządzenia 2016/679 – projektodawca dokonał ponownej analizy wszystkich argumentów przemawiających za czynieniem numeru PESEL daną jawną, czy za nakładaniem na podmioty danych obowiązku udostępnienia a na administratorów obowiązków pozyskiwania numeru PESEL celem identyfikacji osoby, wprowadzania tej danej do rejestrów, w tym państwowych. Powyższa uwaga powinna być uwzględniona przez projektodawcę w sytuacji przetwarzania numeru PESEL, projektodawca powinien analizować zasadność i niezbędność, celowość, jak i adekwatność przetwarzania tej danej osobowej.

**8. Dyrektywa 2016/680.** W projekcie ustawy o ochronie danych osobowych (art. 20 ust. 2) przewidziano, że Prezes Urzędu Ochrony Danych Osobowych będzie organem nadzorczym również w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016, s. 89). Do tej pory jednak Generalny Inspektor Ochrony Danych

Osobowych nie uzyskał żadnych informacji na temat stanu prac legislacyjnych mających na celu implementację przepisów tej dyrektywy do polskiego porządku prawnego. Pamiętać należy, że termin na przyjęcie odpowiednich regulacji w tym zakresie mija dnia 6 maja 2018 r. Z projektu ustawy - Przepisy wprowadzające ustawę o ochronie danych osobowych nie wynika aby uwzględniała ona zmiany w przepisach sektorowych w tym zakresie. Należy przypomnieć, że obecnie Biuro nie dysponuje odpowiednimi narzędziami i zasobami pozwalającymi na realizację zadań wynikających z przepisów dyrektywy 2016/680, w związku z czym niezbędna jest koordynacja prac w tym zakresie z Ministrem Spraw Wewnętrznych i Administracji oraz włączenie w te prace Generalnego Inspektora.

#### **9. Zmiana ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2017 r. poz. 1201)**

W odniesieniu do art. 2 projektu - wyłączeń zaproponowanych w art. 36 § 4 ustawy o postępowaniu egzekucyjnym w administracji – należy przypomnieć, iż prawodawca unijny umożliwia państwom członkowskim ograniczenie zastosowania art. 12 – 22, art. 34 oraz art. 5 rozporządzenia 2016/679, jedynie w przypadkach opisanych w art. 23 ust. 1. Brak jest zatem dowolności projektodawcy w zakresie możliwości wyłączenia zastosowania ww. przepisów przez ustawodawcę krajowego, tak jak w komentowanym przypadku.

Wskazać należy, że ustawodawca krajowy może ograniczyć zastosowanie ww. przepisów jedynie jeżeli:

- 1) ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz
- 2) jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:
  - a) bezpieczeństwu narodowemu;
  - b) obronie;
  - c) bezpieczeństwu publicznemu;
  - d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
  - e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;
  - f) ochronie niezależności sądów i postępowania sądowego;



- g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;
- h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) – e) oraz g);
- i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
- j) egzekucji roszczeń cywilnoprawnych.

Projektodawca w uzasadnieniu do projektu, wskazał, że zdecydował się na wyłączenie zastosowania art. 12 – 22 i art. 34 rozporządzenia 2016/679 w zakresie niezbędnym do realizacji zadań publicznych przez organy egzekucyjne i wierzycieli. Wskazać należy, że wykonanie obowiązków określonych w art. 12 – 22 i art. 34 rozporządzenia 2016/679 nie stoi w sprzeczności z realizacją zadań publicznych przez organy egzekucyjne i wierzycieli w postępowaniu egzekucyjnym w administracji. Wyłączenie obowiązków organów egzekucyjnych oraz podmiotów publicznych będących wierzycielami, nie jest również niezbędne dla wykonywania zadań przez te podmioty. Zaznaczyć należy, że w toku postępowania egzekucyjnego strony tego postępowania, w tym również osoby fizyczne, pozyskują część informacji wskazywanych w art. 14 i art. 16 rozporządzenia 2016/679, w związku z czynnościami, które podejmują organy egzekucyjne i wierzyciele (np. wezwanie do wykonania obowiązku przed wszczęciem egzekucji, przedstawienie tytułu wykonawczego). Ponadto częściowo obowiązki określone w art. 12-22 są realizowane przez organy egzekucyjne i wierzycieli w ramach postępowania egzekucyjnego lub są możliwe do zrealizowania w ramach uprawnień stron tego postępowania (w tym, art. 14 ust. 1 lit. a, c, d., art. 15, art. 16 rozporządzenia 2016/679).

Przepisy powszechnie obowiązujące gwarantują również częściową realizację art. 17 – art. 20 rozporządzenia 2016/679).

Wierzyciele oraz organy egzekucyjne są podmiotami publicznymi, które przetwarzają dane jedynie w celu realizacji zadań wynikających z przepisów powszechnie obowiązujących. W przypadku zakończenia postępowania egzekucyjnego, materiały zgromadzone w aktach postępowania egzekucyjnego są archiwizowane zgodnie z ustawą o narodowym zasobie archiwalnym i archiwach, w związku z czym art. 17 ust. 1 i 2 rozporządzenia 2016/679 nie miałyby zastosowania do tych podmiotów, zgodnie z art. 17 ust. 3 lit. d rozporządzenia.

Z uwagi na to, że podmioty publiczne w ramach postępowania egzekucyjnego nie mogą przetwarzać danych w innych celach niż realizacja zadań ustawowych, art. 18 ust. 1 rozporządzenia

2016/679 nie będzie miał praktycznego zastosowania w postępowaniu egzekucyjnym, z uwagi na art. 18 ust. 2 ww. aktu.

W przypadku kwestionowania prawidłowości przetwarzanych danych (art. 18 ust. 1 lit. a rozporządzenia 2016/679 strona, w ramach postępowania egzekucyjnego, jest uprawniona do dokonywania aktualizacji swoich danych. W przypadku przetwarzania nieaktualnych danych, strona ma prawo do skorzystania z środków przewidzianych w zmienianej ustawie (np. podważenia tytułu wykonawczego).

Informacje określone w art. 19 rozporządzenia 2016/679 są udzielane stronie w ramach postępowania egzekucyjnego, przy okazji kierowania do niej korespondencji.

Przepisy zmienianej ustawy przewidują możliwość uzyskiwania przez strony postępowania egzekucyjnego odpisów i kopii akt oraz zaświadczeń, w związku z czym, uznać należy, że realizacja ww. przepisu jest uregulowana przez ustawodawcę krajowego, co stanowi realizację uprawnień gwarantowanych art. 20 rozporządzenia 2016/679.

Prawodawca unijny umożliwi państwom członkowskim ograniczenie zastosowania art. 12 – 22, art. 34 oraz art. 5 rozporządzenia 2016/679, jednakże jedynie w przypadkach opisanych w art. 23 ust. 1 oraz jeżeli przepisy powszechnie obowiązujące zawierają regulację, w stosownym przypadku:

- a) celach przetwarzania lub kategorii przetwarzania;
- b) kategoriach danych osobowych;
- c) zakresie wprowadzonych ograniczeń;
- d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;
- e) określeniu administratora lub kategorii administratorów;
- f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;
- g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz
- h) prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Przepisy ustawy o postępowaniu egzekucyjnym w administracji określają cel przetwarzania danych osobowych oraz zakres tych danych. Przewidują również sposób dostępu do akt postępowania egzekucyjnego (zgodnie z ustawą z dnia 14 czerwca 1960 r. - Kodeks postępowania

administracyjnego (Dz. U. z 2017 r. poz. 1257), katalog podmiotów uprawnionych, mających dostęp do akt postępowania egzekucyjnego, oraz określają organ egzekucyjny, który jest jednocześnie administratorem, z uwagi na realizację zadań ustawowych. Natomiast przepisy ustawy z 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. 2016 r. poz. 1506, 1948 oraz z 2017 r. poz. 1086) regulują okresy oraz sposób przechowywania akt postępowania egzekucyjnego po zakończeniu tego postępowania, a tym samym zawartych w nich danych osobowych.

W uzasadnieniu wskazano, że wprowadzany przepis został uzupełniony ponadto o wymaganą przez przepisy unijne regulację zobowiązującą administratora do wdrożenia odpowiednich zabezpieczeń zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu danych osobowych. W projektowanym przepisie brak jest jednak tego rodzaju uregulowania. Ponadto, w uzasadnieniu wskazano również, że osoby, których dane dotyczą, mają prawo uzyskania od administratora informacji, o powyższych ograniczeniach, o ile nie narusza to celu ograniczenia. W projektowanym przepisie brak jest jednak uregulowania tej kwestii.

Prawodawca unijny w art. 23 ust. 2 lit. g rozporządzenia 2016/679 przewidział również obowiązek wskazywania w przepisach powszechnie obowiązujących ryzyka naruszenia praw lub wolności osób, których dane dotyczą, czego brak w projektowanym przepisie. Podkreślić należy, że wprowadzanie ograniczeń w zakresie art. 12 - 22 i 34 rozporządzenia 2016/679, z pominięciem wskazania elementów określonych w art. 23 ust. 2, oznaczać będzie niedopuszczalność wyłączenia ww. przepisów rozporządzenia.

W odniesieniu do proponowanego wyłączenia art. 34 rozporządzenia 2016/679 wskazać należy, że obowiązek zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych nie stoi w sprzeczności, z realizacją zadań publicznych przez organy egzekucyjne i wierzycieli. Zawiadomienie takie bowiem nie ma wpływu na podejmowanie działań przez administratora, w toku postępowania egzekucyjnego. Wykonanie obowiązku określonego w art. 34 nie utrudnia prowadzenia postępowania egzekucyjnego, zarówno z perspektywy wierzyciela, jak i organu egzekucyjnego. Strona nie uzyskuje również informacji, których udostępnienie będzie sprzeczne z realizowanymi zadaniami przez podmioty zobowiązane. Podnieść należy, że projektodawca nie wskazał z jakich powodów zdecydował się na wprowadzenie proponowanych wyłączeń oraz nie uzasadnił ich konieczności.

#### **10. Zmiana ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku ochrony Rzeczypospolitej Polskiej (Dz. U. z 2016 r. poz. 1534)**

W art. 3 projektu ustawy wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi wyłączenie z ww. stosowania art. 12 rozporządzenia 2016/679. Wyjaśnienia wymaga wyłączenie z przepisów przedmiotowej ustawy art. 12 ust 3 - 4 a także art. 13, 14, 17 - 22 oraz art. 34 rozporządzenia 2016/679. Ponadto projektodawca powinien wskazać w przepisach ustawy jaki jest cel wszystkich przedmiotowych wyłączeń oraz wypełnić obowiązki z art. 23 ust. 2 rozporządzenia. Przedstawione wyżej argumenty w kwestii wyłączeń poszczególnych przepisów rozporządzenia pozostają aktualne.

#### **11. Zmiana ustawy z dnia 29 maja 1974 r. o zaopatrzeniu inwalidów wojennych i wojskowych oraz ich rodzin (Dz. U. z 2016 r. poz. 871 i 2138 oraz z 2017 r. poz. 2)**

W dodawanym do art. 50a ust. 3a ww. ustawy nie został wprost wskazany cel wyłączenia art. 12 ust. 3 i 4, art. 13, art. 14, art. 17 – 22 i art. 34 rozporządzenia 2016/679. Jeżeli projektodawca widzi potrzebę wyłączenia wskazanych przepisów rozporządzenia to powinien nie tylko jasno wskazać przyczynę wyłączenia lecz również spełnić warunki, którym powinien odpowiadać akt prawny zawierający takie wyłączenia z art. 23 ust. 2 lit. a – h. Aktualne w zakresie wyłączeń proponowanych przez projektodawcę pozostają uwagi wniesione do zmiany ustawy o postępowaniu egzekucyjnym w administracji.

#### **12. Zmiana ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2016 r., poz. 1666, 2138 i 2255 oraz z 2017 r. poz. 60 i 962)**

W art. 5 projektu ustawy rozważenia wymaga, czy rzeczywiście niezbędne jest żądanie (czyli pozyskiwanie na zasadzie obowiązku) od osoby ubiegającej się o zatrudnienie adresu do korespondencji oraz adresu poczty elektronicznej albo numeru telefonu (art. 22<sup>1</sup> §1 pkt 3 i 4 Kodeksu pracy). Jako że nie można narzucić osobie ubiegającej się o zatrudnienie posiadania poczty elektronicznej czy telefonu, sugeruje się połączenie pkt. 3 i 4 oraz zastąpienie ich ogólnym sformułowaniem „dane kontaktowe” – z zastrzeżeniem, iż decyzja, jakie będą to dane, należeć będzie do pracownika.

Możliwość żądania przez pracodawcę udokumentowania danych osobowych, jeżeli uzna za konieczne ich potwierdzenie (art. 22<sup>1</sup> §3) sformułowana jest, w opinii Generalnego Inspektora, w sposób zbyt szeroki i powinna zostać ograniczona do obiektywnych kryteriów, tak aby zapobiec arbitralnym działaniom pracodawcy w tym zakresie. Żądanie udokumentowania danych osobowych powinno być zatem możliwe wyłącznie wtedy, kiedy jest to konieczne, *ergo* – wynika z

przepisów prawa. Zaproponowana treść art. 22<sup>1</sup> §4 stanowi w opinii GODO zbędne powtórzenie ogólnej zasady minimalizacji danych wyrażonej w art. 5 ust. 1 lit. c rozporządzenia 2016/679.

Wobec braku odniesienia się w uzasadnieniu do projektu do zaproponowanego kształtu art. 22<sup>1</sup> § 5, Generalny Inspektor Ochrony Danych widzi konieczność wyjaśnienia przez projektodawcę *ratio legis* tej regulacji.

Projektowany art. 22<sup>2</sup> §1 zawiera szerokie upoważnienia do przetwarzania za zgodą pracownika – czynienia na danych wszelkich operacji, w tym np. ich pozyskiwania czy udostępniania – przez pracodawcę bliżej nieokreślonego katalogu/zakresu danych osobowych, na dodatek „dotyczących stosunku pracy”, co w żaden sposób nie precyzuje jakiego rodzaju mogą to być informacje, z jakich źródeł mogą pochodzić, ani na jakim etapie mogą mieć one miejsce (czy także podczas trwania stosunku pracy?).

Odnosząc się do kwestii dopuszczalności przetwarzania danych przez pracodawcę również w oparciu o wyrażoną przez pracownika zgodę, zauważyć należy, iż wynika ona wprost z motywu 155 rozporządzenia 2016/679. Motyw ten przewiduje możliwość uregulowania w prawie państwa członkowskiego warunków, na których dane osobowe w związku z zatrudnieniem można przetwarzać za zgodą pracownika do celów procedury rekrutacyjnej, wykonywania umowy o pracę, w tym wykonywania obowiązków określonych w przepisach lub w porozumieniach zbiorowych, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

Zaproponowanych przez projektodawcę przepisów (art. 22<sup>2</sup> §1-5) nie można jednak uznać za czyniące zadość tym wytycznym.

Korzystanie z przesłanki zgody nie budzi wątpliwości w sytuacji, gdy osoba ubiegająca się o zatrudnienie lub pracownik z własnej inicjatywy i świadomie przekazują dane pracodawcy z zakresie szerszym niż przewidują to przepisy prawa, bowiem już obecnie jest to powszechnie stosowaną praktyką, zwłaszcza na etapie rekrutacji.

Zastanowić się jednak należy nad innymi przypadkami przetwarzania danych na podstawie zgody wyrażonej przez osobę ubiegającą się o zatrudnienie lub pracownika. Zgodnie z projektowanym art. 22<sup>2</sup> §4 przetwarzanie w oparciu o przesłankę zgody może dotyczyć danych osobowych udostępnianych na wniosek pracodawcy. Nie sprecyzowano jednak, do kogo taki wniosek może być skierowany, co rodzi ryzyko rozszerzającej wykładni tego przepisu i wykorzystywania go do przeprowadzania tzw. *background screeningu*. Tego rodzaju praktyka

wydaje się, zdaniem Generalnego Inspektora, nadmierną ingerencją w prywatność jednostki, nieznajdującą obecnie podstaw w powszechnie obowiązujących przepisach prawa, nieuzasadniona jest zatem jej pośrednia legalizacja poprzez tak ogólne sformułowanie art. 22<sup>2</sup> §4.

Sugeruje się zatem zawężenie możliwości pozyskiwania danych osobowych na podstawie zgody do sytuacji udostępniania ich z własnej inicjatywy pracownika (osoby ubiegającej się o zatrudnienie), a także na żądanie pracodawcy skierowane do pracownika, ale wyłącznie wtedy, gdy pozyskanie danych w szerszym zakresie jest niezbędne dla realizacji praw i obowiązków wynikających ze stosunku pracy.

Pamiętać bowiem należy, iż zgoda na przetwarzanie danych musi być dobrowolna, konkretna i świadoma. Innymi słowy, chodzi o to, aby podmiot danych mógł swobodnie wyrazić przyzwolenie (lub nie) na konkretny sposób wykorzystania lub ujawnienia jego danych osobowych, bez żadnej presji lub przymusu. Zostało to podkreślone w motywie 43 rozporządzenia 2016/679, stanowiącym, że „Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem(...)”. Odmowa zgody nie może powodować negatywnych implikacji dla podmiotu danych. Wprawdzie projektodawca wskazał tę przesłankę w projekcie zmian przepisów, jednakże z uwagi na brak równowagi stron, pracownicy prawie nigdy nie są w stanie swobodnie wyrażać lub odmawiać zgody, biorąc pod uwagę zależność wynikającą z relacji pracodawca/pracownik.

Dodać trzeba jednocześnie, że biorąc pod uwagę treść art. 7 ust. 3 rozporządzenia 2016/679, pracownik musiałby mieć zagwarantowane prawo do wycofania zgody w dowolnym momencie, które również nie mogłoby powodować dla niego jakichkolwiek negatywnych konsekwencji.

Zaproponowana w art. 22<sup>2</sup> § 1 Kodeksu pracy możliwość przetwarzania przez pracodawcę danych biometrycznych budzi duże zastrzeżenia. Po pierwsze, rozporządzenie 2016/679 zalicza dane biometryczne do tzw. szczególnych kategorii danych osobowych. Art. 9 ust. 1 rozporządzenie 2016/679 wprowadza generalny zakaz przetwarzania danych szczególnych kategorii (w tym biometrycznych), za wyjątkiem sytuacji enumeratywnie wskazanych. Jedną z przesłanek dopuszczających przetwarzanie takich danych jest zgoda osoby spełniająca warunki określone w rozporządzeniu 2016/679. Ze względu na użycie sformułowania „przetwarzanie przez pracodawcę danych biometrycznych obejmuje tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy” powstają istotne wątpliwości, o jakie dane chodzi, tj. jakie dane biometryczne dotyczą stosunku pracy. Przepis nie wskazuje również, w jakich przypadkach dane te będą wymagane i

przetwarzane. Należy zwrócić uwagę, iż pracownik w stosunku pracy nie jest równorzędną stroną. Szczególnie zatem w tej dziedzinie, tak jak dotychczas, rolą ustawodawcy jest stworzenie gwarancji ochrony praw osób, których dane są przetwarzane. Zgodnie z rozporządzeniem 2016/679 należy dążyć do minimalizacji przetwarzanych danych, w tym danych pracowników oraz respektować zasadę ograniczenia celu.

Dotychczasowe podejście w tym zakresie akcentowało zasadę, że zbieranie danych biometrycznych od pracownika może mieć zastosowanie tylko w przypadkach, gdy będzie to niezbędne i adekwatne do celu. Swobodna zgoda w relacjach pracodawca-pracownik jest wątpliwa z uwagi na brak równowagi stron. Ponadto pracodawca powinien dążyć do stosowania wobec pracownika środków jak najmniej ograniczających jego prawa i wolności.

Wskazane kwestie były przedmiotem rozważań Grupy Roboczej Art. 29 m.in. w opinii nr 2/2017 w sprawie przetwarzania danych w pracy (WP 249)<sup>1</sup>: „...każdy pracodawca powinien zadać sobie pytanie, czy konieczne jest przetwarzanie tego typu danych dla osiągnięcia celu. Wprowadzenie regulacji zezwalająca na pobieranie od pracownika odcisków palców, tęczę oka, w tak ogólnej formie bez wskazania, iż powinna być ona stosowana w wyjątkowych sytuacjach, podyktowanych szczególnymi względami. Pracodawca powinien korzystać z biometrii w przypadkach gdy nie da się w inny sposób osiągnąć celu. Ta kwestia powinna ulegać wyważeniu w odniesieniu do konkretnych okoliczności”.

Ponadto kwestiami tymi zajmowały się również polskie sądy administracyjne, m.in. Naczelny Sąd Administracyjny: „Skoro zasada proporcjonalności wyrażona w art. 26 ust. 1 pkt 3 ustawy z 1997 r. o ochronie danych osobowych jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników zatrudnionych w urzędzie skarbowym jest nieproporcjonalne do zamierzonego celu ich przetwarzania. W ocenie Sądu wyrażona na prośbę pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych, narusza prawa pracownika i swobodę wyrażenia przez niego woli. Za takim stanowiskiem przemawia zależność pracownika od pracodawcy. Brak równowagi w relacji pracodawca - pracownik stawia pod znakiem zapytania dobrowolność w wyrażeniu zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). W przyjętym przez Grupę w dniu 1 sierpnia 2003 r. dokumencie roboczym w sprawie biometrii przyjęto jako niezbędną zasadę proporcjonalności i legalności. Oznacza to, że ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności

---

<sup>1</sup> [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=45631](http://ec.europa.eu/newsroom/document.cfm?doc_id=45631), <http://giodo.gov.pl/pl/1520296/10060>

wyrażona w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników zatrudnionych w Urzędzie Skarbowym w Z. jest nieproporcjonalne do zamierzonego celu ich przetwarzania. We wspomnianym dokumencie z dnia 1 sierpnia 2003 r. Grupa Robocza stwierdziła, że "pracodawca popełnia błąd, jeśli próbuje zalegalizować przetwarzanie danych pochodzących od pracownika za pomocą uzyskanej od pracownika zgody. Można posłużyć się zgodą, jeśli odnosi się ona do przypadku, w którym pracownik ma całkowitą swobodę jej udzielenia i może odmówić udzielenia takiej zgody bez poniesienia szkody". Naczelny Sąd Administracyjny w pełni aprobuje pogląd wyrażony w dokumencie Grupy Roboczej" (I OSK 1476/10).

Trzeba również podkreślić, że projektodawca nie uwzględnił, że dostęp do ww. danych w tym danych biometrycznych, oprócz pracodawcy w praktyce będą miały również podmioty świadczące na rzecz pracodawcy obsługę czytników np. linii papilarnych.

Jeśli miałyby dochodzić do przetwarzania danych biometrycznych pracownika, to niezbędne jest wskazanie zindywidualizowanych celów pracodawcy, dla realizacji których takie szczególne kategorie danych jak dane biometryczne, mogłyby być przetwarzane a także doprecyzowanie rodzajów (kategorii) takich danych. Oczywiście, wskazanie takich celów i kategorii danych biometrycznych jest możliwe jedynie po wykazaniu przez projektodawcę, że ich realizacja nie może być osiągnięta w inny sposób, mniej ingerujący w prawa i wolności pracownika.

Generalny Inspektor stoi zatem na stanowisku, iż dopuszczalność przetwarzania danych biometrycznych pracowników powinna zostać uregulowana w sposób bardziej szczegółowy i ograniczona – biorąc pod uwagę wspomnianą wyżej zasadę minimalizacji danych – do specyficznych sytuacji, w których przetwarzanie danych biometrycznych może być uzasadnione kontrolą dostępu do określonych pomieszczeń czy informacji, w sytuacji gdy nie można takiego celu osiągnąć metodami mniej inwazyjnymi.

Wówczas pozyskiwanie takich danych przez pracodawcę mogłoby odbywać się w oparciu o przepis prawa, np. tak jak w ogólnym założeniu zostało to zaproponowane w art. 41 projektu–ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2016 r. poz. 1988, z późn. zm.), art. 13c ust. 2 : „Bank ma prawo żądać od pracownika danych biometrycznych, w szczególności w postaci odcisków palców, głosu, obrazu rogówki i sieci żył palców, jeżeli podanie takich danych jest konieczne ze względu na kontrolę dostępu do informacji przetwarzanych przez bank i pomieszczeń.” Do treści tego przepisu Generalny Inspektor odnosi się poniżej. Innym



rozwiązaniem mogłoby być regulowanie kwestii przetwarzania danych biometrycznych w stosunkach pracy wyłącznie w przepisach sektorowych.

W projektowanej nowelizacji Kodeksu pracy nie zostało wskazane jakie rodzaje danych biometrycznych mogą być przetwarzane przez pracodawcę, a także w jakim kontekście i w jakich celach ich przetwarzanie może mieć miejsce. Zauważyć należy, iż zwłaszcza jeśli np. dane biometryczne będą przetwarzane w wielkoskalowych systemach informatycznych z użyciem innych nowych technologii takich jak np. rozpoznawanie indywidualnych cech twarzy czy skan tęczówki oka, może to powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W związku z powyższym przetwarzanie danych biometrycznych powinno być możliwe tylko tam, gdzie jest to niezbędne. Do przypadków takich można zaliczyć między innymi:

- 1) Wydawanie środków identyfikacji elektronicznej, dla których tzw. rozporządzenie eIDAS<sup>2</sup> wymaga zapewnienia wysokiego poziomu bezpieczeństwa, w tym potwierdzenia tożsamości osoby poprzez dowody identyfikacji fotograficznej lub biometrycznej zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2015/1502<sup>3</sup>;
- 2) Wydawanie dokumentów podróży (paszportów) i dokumentów tożsamości;
- 3) Dostępu do ściśle strzeżonych pomieszczeń (systemów) wymagających wysokiego poziomu bezpieczeństwa, w tym potwierdzenia tożsamości osoby poprzez dowody identyfikacji fotograficznej lub biometrycznej.

Proponowane zmiany nie wskazują takich potrzeb, co może prowadzić do zbyt szerokiego wykorzystywania danych biometrycznych, w tym również tam, gdzie nie występuje duże ryzyko narażenia administratora na straty materialne lub niematerialne, jak np. do kontroli czasu pracy, gdzie można zastosować szereg innych metod kontroli mniej ingerujących w prywatność.

Dodatkowo należy podnieść, iż zaproponowane zmiany nie uwzględniają zawartego w rozporządzeniu 2016/679 w odniesieniu do szczególnych kategorii danych obowiązku przeprowadzenia oceny skutków dla ochrony danych.

---

<sup>2</sup> rozporządzenie PE i R (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. UE. L. z 2014 r. Nr 257, str. 73-114)

<sup>3</sup> rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Tekst mający znaczenie dla EOG), (Dz. U. UE. L. z 2015 r. Nr 235, str. 7-20)

Projektodawca nie wykorzystał zarówno tutaj, jak i w odniesieniu do zmian w innych przepisach sektorowych, możliwości jakie niesie ze sobą regulacja z art. 35 ust. 10 rozporządzeniu 2016/679. Przepis ten znosi obowiązek dokonania takiej oceny skutków dla ochrony danych, jeśli oceny tej dokonał ustawodawca już na etapie projektu w ramach oceny skutków regulacji w związku z przyjęciem danej podstawy prawnej przetwarzania. Ocena skutków regulacji projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych – nie zawiera takiej oceny.

Przepis ten również umożliwia państwom członkowskim wskazanie wprost w przepisach prawa, że niezbędne jest dokonanie oceny skutków dla ochrony danych przed podjęciem czynności przetwarzania z czego projektodawca również nie skorzystał. Należy zatem mieć świadomość, że pomimo wprowadzonej w ww. przepisach podstawy prawnej, przetwarzanie danych biometrycznych we wskazanych obszarach będzie niemożliwe, jeśli ocena skutków dla ochrony danych wykonana przez administratora wykaże wysokie ryzyko naruszenia praw i wolności osób, których dane są przetwarzane, a organ nadzorczy w wyniku konsultacji w trybie art. 36 rozporządzenia 2016/679 uzna, że przetwarzanie to naruszałoby przepisy rozporządzenia.

W 22<sup>2</sup> § 5 Kodeksu pracy wyłączona została możliwość przetwarzania danych osobowych o nałogach, o stanie zdrowia oraz o życiu seksualnym lub orientacji seksualnej nawet za zgodą pracownika. Uzasadnienie nie wyjaśnia jednak, dlaczego to właśnie takie, a nie inne, kategorie danych osobowych zdecydowano się objąć przedmiotowym wyłączeniem, nie zakazując jednocześnie przetwarzania np. danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne czy też przynależność do związków zawodowych. Wskazane byłoby zatem bardziej szczegółowe odniesienie się do tej kwestii przez projektodawcę.

Projektodawca w 22<sup>2</sup> § 6 Kodeksu pracy zobowiązuje ministra właściwego do spraw informatyzacji do określenia, w drodze rozporządzenia, sposobu przetwarzania danych biometrycznych uwzględniając zapewnienie ochrony przetwarzanych danych biometrycznych odpowiedniej do zagrożeń. Delegacja ta została sformułowana w sposób na tyle ogólny, iż nie jest jasne, czy wydany akt wykonawczy miałby dotyczyć wyłącznie przetwarzania danych biometrycznych pracowników. Przypomnieć w tym kontekście należy art. 92 ust. 1 Konstytucji RP, zgodnie z którym rozporządzenia wydawane są na podstawie szczegółowego upoważnienia zawartego w ustawie i w celu jej wykonania – a zatem nie mogą dotyczyć innych niż nowelizowana ustawa celów przetwarzania danych.

Uzasadnione byłoby również – z uwagi na istniejące już obecnie wątpliwości interpretacyjne – doprecyzowanie z jakich przepisów może wynikać prawo do żądania przez pracodawcę podania danych osobowych w zakresie szerszym, niż pozwalają na to przepisy Kodeksu pracy (*vide* art. 22<sup>3</sup> §1). Art. 9 § 1 do źródeł prawa pracy zalicza przepisy Kodeksu pracy oraz przepisy innych ustaw i aktów wykonawczych, określające prawa i obowiązki pracowników i pracodawców, a także postanowienia układów zbiorowych pracy i innych opartych na ustawie porozumień zbiorowych, regulaminów i statutów określających prawa i obowiązki stron stosunku pracy. Nie jest zatem jasne, czy „przepisy prawa”, o których mowa w art. 22<sup>3</sup> §1 dotyczą wszystkich tych aktów, czy jedynie powszechnie obowiązujących przepisów rangi ustawy.

W projektowanym art. 22<sup>4</sup> przewidziana została możliwość stosowania przez pracodawcę – w określonych w tym przepisie celach – środków technicznych umożliwiających rejestrację obrazu, tj. monitoringu. Przywołać w tym kontekście należy wspomniany wyżej obowiązek dokonania oceny skutków dla ochrony danych i wiążące się z nim konsekwencje.

Nie jest ponadto jasne, w jaki sposób miałyby być weryfikowana kwestia, czy monitoring wizyjny nie stanowi środka kontroli wykonywania przez pracownika zadań – zwłaszcza w sytuacji, gdy wideonadzór ma na celu zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, cel ten jest bowiem związany w sposób bezpośredni z właściwą realizacją przez pracownika jego obowiązków.

Zachodzi jednocześnie potrzeba rozważenia, czy w przepisach nie powinna zostać uregulowana kwestia dopuszczalności albo zakazu stosowania innych form monitoringu, w tym rejestracji dźwięku czy monitorowania poczty elektronicznej. Dotychczas Generalny Inspektor stał na stanowisku, iż pracodawca – co do zasady – ma prawo kontrolować pracowników, ale musi przy tym uwzględniać gwarantowane im przepisami Konstytucji RP i Kodeksu cywilnego prawo do prywatności i poszanowania dóbr osobistych, do czego zobowiązuje go m.in. art. 11<sup>1</sup> Kodeksu pracy. Ponadto ma prawo kontrolować, co pracownicy robią w godzinach pracy, w tym – do czego wykorzystują udostępnione im narzędzia. Jednak w każdym przypadku, gdy pracodawca zdecyduje się na kontrolowanie pracowników, powinien poinformować pracownika o zakresie i celu prowadzonej kontroli. Informacja taka powinna zostać przekazana przed rozpoczęciem działań kontrolnych. Dopuszczalne jest także, by pracodawca w celu ochrony tajemnicy przedsiębiorstwa zabronił pracownikom korzystania z Internetu, poczty elektronicznej czy telefonu do celów innych niż służbowe i zastrzegł sobie prawo do kontrolowania również treści przesyłek czy rozmów. Jednak może tak postąpić tylko wtedy, gdy pracownik zostanie o tym uprzednio poinformowany, a

nie dopiero wtedy, gdy pracodawca uzna, że nastąpiło przekroczenie zasad, które w przedsiębiorstwie obowiązują. Kwestie te nie są jednak uregulowane w przepisach w sposób wyraźny, a zatem w opinii Generalnego Inspektora projektodawca powinien się do nich odnieść w obecnie trwających pracach legislacyjnych.

Rozważenia wymaga również szersze sformułowanie katalogu pomieszczeń, które nie mogą być objęte monitoringiem wizyjnym i uwzględnienie wśród nich w szczególności pomieszczeń udostępnionych zakładowym organizacjom związkowym art. 22<sup>4</sup> § 2).

Wskazany w art. 22<sup>4</sup> § 3 okres retencji danych sformułowany został w sposób nieprecyzyjny, stanowi bowiem w istocie powtórzenie zasady ogólnej. Niezrozumiałe – i trudne do zastosowania w praktyce – jest ponadto objęcie nim wyłącznie danych osobowych, a nie pełnych nagrań z monitoringu.

Zaproponowana w art. 22<sup>4</sup> § 4 forma poinformowania o wprowadzeniu monitoringu wydaje się być niewystarczająca. Biorąc pod uwagę, iż w wyniku stosowania monitoringu dochodzić będzie również do przetwarzania danych osobowych osób trzecich, tym bardziej konieczne wydaje się odpowiednie oznaczenie miejsc objętych rejestracją obrazu.

Wskazać przy tym należy na Opinię Grupy Roboczej art. 29 nr 4/2004<sup>4</sup>, w której zwrócono uwagę m. in. na konieczność respektowania zasady proporcjonalności (dane muszą być adekwatne i istotne dla celów przetwarzania) przy posługiwaniu się wideonadzorem, która oznacza przede wszystkim, że urządzenia monitoringu wizyjnego mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, nie wymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami.

Istotne znaczenie ma w tej materii – jak dalej traktuje ww. opinia – realizacja obowiązku informacyjnego wobec osób, których dane osobowe pozyskane zostały za pomocą monitoringu wizyjnego, zgodnie z wymogami art. 10 i 11 ww. Dyrektywy 95/46/WE. Wskazano przy tym, iż osoby te muszą mieć świadomość faktu prowadzenia czynności wideonadзору, tablice informacyjne o monitoringu wizyjnym powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Muszą także wskazywać cele działań

---

<sup>4</sup> [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf),  
<http://www.giodo.gov.pl/pl/1520189/7146>

nadzoru jak również administratora przetwarzania, natomiast wymiary tablic muszą być proporcjonalne do miejsca, w którym są umieszczone.

Aktualne w tym zakresie pozostają uwagi Generalnego Inspektora poczynione w toku prac nad projektem założeń do ustawy o monitoringu wizyjnym.<sup>5</sup> Nadal postulatem organu ds. ochrony danych osobowych jest kompleksowe uregulowanie monitorowania przestrzeni przy pomocy kamer w akcie rangi ustawowej.

### **13. Zmiana ustawy z dnia 17 grudnia 1974 r. o uposażeniu żołnierzy niezawodowych (Dz. U. z 2016 r. poz. 616 i 2138)**

W art. 6 projektu ustawy projektodawca poprzez dodanie do art. 4 ust. 1d dokonuje następujących wyłączeń:

- 1) obowiązków informacyjnych (art. 12 ust. 3 i 4, art. 13, art. 14 rozporządzenia 2016/679)
- 2) prawa do usunięcia danych (art. 17 RODO), ograniczenia przetwarzania (art. 18 rozporządzenia 2016/679), obowiązku poinformowania o usunięciu i ograniczeniu (art. 19 rozporządzenia 2016/679), przenoszenia danych (art. 20 rozporządzenia 2016/679), sprzeciwu (art. 21 rozporządzenia 2016/679), automatyczne podejmowanie decyzji (art.22),
- 3) zawiadomienia osoby o naruszeniu ochrony danych osobowych (art. 34 rozporządzenia 2016/679)

W opinii Generalnego Inspektora w przepisie art. 4 ust. 1d nie został wprost wskazany cel wyłączenia ww. przepisów. Interpretacja nowego brzmienia art. 4 zawierającego ust. 1d wskazuje, że dane osobowe żołnierzy, byłych żołnierzy i osób wskazanych w art. 4 ust. 1b – 1bb będą przetwarzane w celu przyznania im nagród i zapomóg. Wydaje się, że – w tej sytuacji – cel wyłączenia przepisów rozporządzenia 2016/679 nie spełnia żadnej z enumeratywnie wymienionych przesłanek z art. 23 ust. 1 lit. a – j aktu unijnego. Jeżeli projektodawca widzi potrzebę wyłączenia tych przepisów to powinien nie tylko jasno wskazać przyczynę wyłączenia lecz również spełnić warunki, którym powinien odpowiadać akt prawny zawierający takie wyłączenia z art. 23 ust. 2 lit. a – h rozporządzenia 2016/679.

### **14. Zmiana ustawy z dnia 21 grudnia 1978 r. o odznakach i mundurach (Dz. U. z 2016 r. poz. 38)**

---

<sup>5</sup> sygn. DOLiS-033-523/13/KK/63260/14 z 13 sierpnia 2014 r., <http://www.giodo.gov.pl/pl/1520293/9914>

W art. 7 projektodawca dodaje art. 4a do ustawy o odznakach i mundurach, który dookreśla administratora przetwarzanych danych w celu nadania odznaki honorowej oraz ewidencjonowania osób wyróżnionych odznaką nie określając przy tym zakresu tych danych w przepisie ustawy. Zakresy danych przetwarzanych w powyższym celu określają załączniki do rozporządzeń wydawanych na podstawie art. 6 ust. 1 tej ustawy będących wnioskami o nadanie odznaki. W związku z powyższym należy w przepisie ustawy określić, że przetwarzanie nie będzie dotyczyć szczególnych kategorii danych osobowych z art. 9 rozporządzenia 2016/679 (z konstrukcji projektowanego przepisu nie wynika czy będą takie dane przetwarzane czy nie) i wskazać taki katalog danych w projektowanym przepisie.

Oprócz powyższych czynności legislacyjnych, zgodnie z zasadami dotyczącymi przetwarzania danych osobowych zawartymi w art. 5 rozporządzenia 2016/679 projektodawca powinien spełnić wymogi zasady minimalizacji danych przy określaniu ich katalogu, zasady prawidłowości, ograniczenia przechowywania oraz integralności i poufności.

#### **15. Zmiana ustawy z dnia 26 stycznia 1982 r. – Karta Nauczyciela (Dz. U. z 2017 r. poz. 1189)**

Należy zauważyć, iż zaproponowana nowelizacja dotyczy wyłącznie szkół artystycznych i placówek prowadzonych lub nadzorowanych przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego. Taka regulacja wydaje się niepełna, zatem Generalny Inspektor wskazuje na potrzebę dokonania przez projektodawcę dodatkowej analizy w tym zakresie. Niezależnie od powyższego, zastrzeżenia organu wzbudzają poniższe kwestie.

Biorąc pod uwagę zasadę minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c rozporządzenia 2016/679 sugeruje się stworzenie zamkniętego katalogu danych, poprzez usunięcie sformułowania „w szczególności” (*vide* proponowane brzmienie art. 91e ust. 1).

Nie jest zrozumiałe generalne uprawnienie do przetwarzania takich danych jak: wykształcenie, miejsce pracy i zajmowane stanowisko, w tym wysokość wynagrodzenia oraz numer rachunku bankowego. Niewątpliwie w indywidualnych przypadkach pozyskiwanie takich danych może być uzasadnione, jednak przepisy powinny takie okoliczności wskazywać, zamiast tworzyć ogólny przepis pozwalający na przetwarzanie tak szczegółowych informacji. Nadmiarowe wydaje się również pozyskiwanie danych w postaci imion rodziców.

Jednocześnie w przypadku przetwarzania danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych – mając na uwadze, że w polskim porządku prawnym nie

istnieje obowiązek posiadania przez osoby fizyczne takich środków komunikacji – należy pozostawić swobodę możliwości podawania takich danych.

Wątpliwości Generalnego Inspektora wzbudzają zaproponowane przez projektodawcę szerokie wyłączenia od stosowania przepisów rozporządzenia 2016/679, polegające na odstąpieniu od stosowania art. 13, art. 14 oraz art. 17-19 ww. aktu w zakresie, w jakim dane są niezbędne do zapewnienie realizacji zadań, o których mowa w ustawie oraz odstąpieniu od stosowania art. 5 ust. 2 rozporządzenia – w zakresie obowiązków wykazywania przestrzegania przepisów art. 5 ust. 1 rozporządzenia. Ponadto projektodawca zdecydował, aby wyłączyć stosowanie art. 34 rozporządzenia, w przypadku, gdy administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej. Ograniczone zostało również stosowanie art. 12 oraz art. 15 rozporządzenia 2016/679.

Wyłączenia powyższe wymagają ponownej weryfikacji i ewentualnego dalszego doprecyzowania, w świetle argumentów przedstawionych powyżej odnośnie art. 2 projektowanej ustawy oraz poniżej do art. 21 oraz art. 28 przepisów wprowadzających.

**16. Zmiana ustawy z dnia 26 maja 1982 r. – Prawo o advokaturze (Dz. U. z 2016 r. poz. 1999 i 2261 oraz z 2017 r. poz. 1139) oraz zmiana ustawy z dnia 6 lipca 1982 r. o radcach prawnych (Dz. U. z 2016 r. poz. 233, 1579 i 2261 oraz z 2017 r. poz. 1139)**

W odniesieniu do art. 9 i 10 projektu, zwrócić uwagę należy na tożsame zastrzeżenia do proponowanych regulacji. Znajdują one także zastosowanie do art. 17 projektu.

Przed wszystkim wątpliwości wzbudza konkretne wskazywanie podmiotów, które pełnią rolę administratora. Jak widać z przedłożonego projektu jest to podyktowane zakresem ustawowo uregulowanych kompetencji i wykonywanych zadań przez te podmioty, jednakże nasuwa się wątpliwość co do zidentyfikowania wszystkich celów przetwarzania danych odpowiadających kompetencjom i obowiązkom administratorów. Zwrócić należy uwagę projektodawcy na okoliczność, iż tak trzeba formułować przepisy by nie dopuścić do zaistnienia w przyszłości ewentualnych problemów z ustaleniem podmiotu odpowiedzialnego za przetwarzanie danych osobowych w konkretnej jednostkowej sytuacji, np. w toku konkretnego postępowania.

Kolejno, zwrócić uwagę należy na wyłączenie przepisów art. 13 – 15 ust. 1 i 3, 18, 19 i 21 rozporządzenia 2016/679, generalnie w stosunku do przetwarzania danych osobowych przez administratorów danych, określonych w odpowiednio w stosunku do adwokatów w art. 16a ust. 1, do radców prawnych w art. 5a ust. 1, w stosunku do notariuszy w art. 78b §1. W nawiązaniu do

ogólnej uwagi zgłoszonej na początku załącznika dotyczącej niezasadnego stosowania ograniczeń - a wręcz wyłączeń - stosowania rozporządzenia 2016/679, o których mowa w art. 23 rozporządzenia 2016/679, wskazać trzeba, że niezgodne z postanowieniami tegoż artykułu rozporządzenia jest dokonywanie całkowitego wyłączenia praw podmiotów danych w sposób sprzeczny z postanowieniami art. 23 rozporządzenia 2016/679. Ewentualną potrzebę ograniczenia stosowania ww. art. 13 – 15 ust. 1 i 3, 18, 19 i 21 rozporządzenia 2016/679 należy nie tylko poprzedzić stosowną analizą powodów wyłączeń, ale przede wszystkim dopuszczalności ich zastosowania. Projektodawca wskazując potrzebą zastosowania ograniczeń powinien nie tylko jasno wskazać ich przyczynę lecz również spełnić warunki, którym powinien odpowiadać akt prawny zawierający takie wyłączenia, stosownie do postanowień art. 23 ust. 2 lit. a – h rozporządzenia 2016/679. Trudno tym samym Generalnemu Inspektorowi nie tylko dostrzec przyczynę ale i zaakceptować dokonanie generalnego zastosowania zaproponowanych rozwiązań w zakresie wyłączeń. Nie wydaje się, aby za przesłankę tego konkretnego ograniczenia mógł być uznany art. 23 ust. 1 pkt g. Oczywiście należy mieć na względzie zasady etyki przy wykonywaniu zawodów zaufania publicznego, ale ograniczenie praw podmiotów danych w każdej sytuacji, także względem klienta korzystającego z usług adwokata/radcy prawnego/notariusza, wzbudza poważne wątpliwości organu do spraw ochrony danych osobowych.

Należy zgłosić również zastrzeżenie do stosowanego w tych ustawach zapisu dotyczącego podleganiu danych osobowych „zabezpieczeniom zapobiegającym nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu wynikającym z procedur prawnych, w których toku są przetwarzane”. Przepis ten bowiem nie wskazuje jakie dokładnie procedury prawne dotyczące zabezpieczeń projektodawca miał na myśli, to znaczy jakie miałyby to być „inne procedury prawne” niż wynikające z rozporządzenia 2016/679. Zwrócić uwagę należy, że procedury zabezpieczeń zapobiegających nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu nie mogą być inne, a tym bardziej węższe czy mniejsze niż wynikające z rozporządzenia 2016/679.

Zastrzeżenie budzi również wyłączenie stosowania art. 58 ust. 1 lit. e i f rozporządzenia 2016/679. Osoby wykonujące ww. zawody nie są zwolnione z obowiązku przestrzegania przepisów o ochronie danych osobowych. Co więcej są one zobligowane do wprowadzenia odpowiednich środków ochrony danych osobowych adekwatnych do zakresu, charakteru przetwarzanych danych oraz do sposobów ich przetwarzania. Wyłączenie stosowania art. 58 ust. 1 lit. e i f rozporządzenia 2016/679 mogłoby bowiem ograniczyć nie tylko możliwości kontrolne organu nadzorczego, ale również wykreować obszary trwale wyłączone spod kontroli zgodności z prawem przetwarzania danych. Do takiej sytuacji dopuścić nie można.



Projektodawca argumentuje wyłączenie ww. artykułu treścią art. 90 rozporządzenia 2016/679, a dokładnie ochroną tajemnicy zawodowej. Jednak nie należy utożsamiać ochrony ww. tajemnicy z uniemożliwieniem kontroli organu nadzorczego w zakresie zgodności przetwarzania danych z przepisami rozporządzenia. Przykładem tego typu sytuacji jest m.in. art. 3 ust. 1 pkt. 3 ustawy z dnia 6 lipca 1982 r. o radcach prawnych, który stanowi, iż *„Obowiązek zachowania tajemnicy zawodowej nie dotyczy informacji udostępnianych na podstawie przepisów ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2014 r. poz. 455 oraz z 2015 r. poz. 1223) - w zakresie określonym tymi przepisami.”* Reasumując istnieje obawa, że wyłączenie art. 58 ust. 1 lit. e i f rozporządzenia 2016/679 ograniczy możliwości kontrolne organu nadzorczego oraz może wykreować obszary trwale wyłączone spod kontroli zgodności z prawem przetwarzania danych.

Analizując dalej przepisy ww. ustaw należy wskazać, że w opinii Generalnego Inspektora doprecyzowania wymaga kwestia przechowywania danych osobowych. Przepisy tych trzech ustaw w sposób lakoniczny i nieprecyzyjny regulują taki okres przechowywania danych, oddając ustalenie tego terminu przez administratora z uwzględnieniem przepisów odrębnych dotyczących terminów. Zgodnie z motywem 39 rozporządzenia 2016/679 aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien zapewnić ograniczenia okresu przechowywania danych do ścisłego minimum, czyli ustalić termin ich usuwania lub okresowego przeglądu. Przyjęcia takiego rozwiązania nie mogą zastępować bliżej niesprecyzowane odesłania do przepisów odrębnych.

#### **17. Zmiana ustawy z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (Dz. U. z 2017 r. poz. 1007)**

W odniesieniu do art. 11 Generalny Inspektor Danych Osobowych ponownie wskazuje (co czynił również na etapie, gdy powstawały przepisy o elektronicznym dostępie do ksiąg wieczystych), że zakres danych osobowych w projektowanym art. 25 ust. 4 oraz w art. 68<sup>2</sup> ust. 5<sup>1</sup>, w tym udostępnianie numeru PESEL, może prowadzić do nadmiernej i nieproporcjonalnej ingerencji w prawa osób, których dane znajdują się w księgach wieczystych. Generalny Inspektor Ochrony Danych Osobowych zauważa, że w obliczu rozpoczęcia stosowania w dniu 25 maja 2018 r. rozporządzenia 2016/679 już dziś dostosowując polskie prawo do ogólnego rozporządzenia o ochronie danych osobowych należy korzystać z pewnych wytycznych w nim zawartych. W świetle rozporządzenia 2016/679 identyfikator osoby musi być poddany szczególnej ochronie, w związku z czym należy stworzyć szczególne gwarancje wynikające z przepisów prawa, mając na względzie

konieczność ich dostosowania do ww. rozporządzenia. Generalny Inspektor sugeruje by obecne unormowania dotyczące jawności numeru PESEL poddać ponownej analizie w świetle zasad przetwarzania danych określonych przepisami rozporządzenia 2016/679: ograniczeniem celu (art. 5 ust. 1 pkt b) oraz minimalizacji danych osobowych (art. 5 ust. 1pkt c), które projektodawca powinien brać pod uwagę, tworząc rozwiązania prawne związane z przetwarzaniem danych osobowych. Na projektodawcy ciąży bowiem odpowiedzialność za ewentualne negatywne konsekwencje proponowanych unormowań, w tym również związane z możliwością naruszenia konstytucyjnie gwarantowanych praw i wolności człowieka i obywatela (m.in. autonomii informacyjnej jednostki, tj. prawa do ochrony danych osobowych – art. 51 Konstytucji RP), jak na przykład kradzież danych, czy niezgodne z zasadami rozporządzenia 2016/679 profilowanie itp.

Powyższa uwaga dotycząca jawności numeru PESEL powinna być uwzględniona przez projektodawcę także w kontekście tworzenia/zmiany innych aktów normatywnych, w których udostępniany jest numer PESEL (np. ustawy o KRS, art. 8 przepisów wprowadzających ustawę o ochronie danych osobowych - Karta Nauczyciela, art. 14 przepisów wprowadzających ustawę o ochronie danych osobowych – ustawa o drogach publicznych, art. 18 przepisów wprowadzających ustawę o ochronie danych osobowych – ustawa o systemie oświaty, art. 27 przepisów wprowadzających ustawę o ochronie danych osobowych – ustawa o fundacji – Zakład Narodowy imienia Ossolińskich, art. 32 przepisów wprowadzających ustawę o ochronie danych osobowych – ustawa o ruchu drogowym). Każdorazowo przy podejmowaniu decyzji o jawności numeru PESEL projektodawca powinien uzasadnić celowość i adekwatność przetwarzania tej danej osobowej, szczególnie gdy numer PESEL jest wymagany w obrocie gospodarczym (gdzie numer PESEL jest zbędny i może być zastąpiony np. numerem dowodu osobistego).

#### **18. Zmiana ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2016 r. poz. 1506, z późn. zm.)**

Uwzględniając, iż o zezwolenie na wywóz za granicę materiałów archiwalnych (art. 14 ust. 2 i 3 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach) może się ubiegać także osoba fizyczna, zaś prawo polskie (poza szczególnymi wypadkami) nie kreuje obowiązku posiadania przez osoby fizyczne telefonu ani posługiwania się pocztą elektroniczną, wydaje się, iż w projektowanym –art. 13 pkt 2 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych – art. 22b ust. 1 pkt 3 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach powinna być pozostawiona swoboda (dobrowolność) w zakresie

podawania przez osoby fizyczne numeru telefonu i adresu poczty elektronicznej. Powstaje również pytanie co oznacza, użyte w tym przepisie, sformułowanie „adres elektroniczny”.

Podobną uwagę zgłosić wypada do art. 22b ust. 2 pkt 3 oraz ust. 4 pkt 2 lit. d i pkt 3 lit. d ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi też pozostawianie w art. 22b ust. 4 pkt 2 i 3 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach otwartego katalogu przetwarzanych danych osobowych poprzez użycie sformułowania „w szczególności”. Zgodnie z zasadą minimalizacji danych, określoną art. 5 ust. 1 lit. c rozporządzenia 2016/679 projektodawca powinien ustanowić zamknięty katalog przetwarzanych danych, adekwatny i ograniczony jedynie do danych niezbędnych do celów, w których są one przetwarzane.

Niezrozumiała jest dyspozycja projektowanego art. 22c ust. 2 ustawy o narodowym zasobie archiwalnym i archiwach, gdyż nie wiadomo do jakiego „przepisu ust. 2” on odsyła.

Zakwestionować należy również art. 22c ust. 3 ustawy o narodowym zasobie archiwalnym i archiwach. Prawodawca unijny w art. 23 ust. 1 rozporządzenia 2016/679, dopuścił m.in. ograniczenie stosowania zasady rozliczalności z art. 5 ust. 2 rozporządzenia unijnego, jednakże obwarował wprowadzenie takiego ograniczenia wymogiem wykazania, iż jest to w demokratycznym społeczeństwie środek niezbędny i proporcjonalny służący: a) bezpieczeństwu narodowemu, b) obronie, c) bezpieczeństwu publicznemu, d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom, e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu, f) ochronie niezależności sądów i postępowania sądowego, g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu, h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)–e) oraz g), i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób, j) egzekucji roszczeń cywilnoprawnych.

W kwestionowanym art. 22c ust. 3 ustawy o narodowym zasobie archiwalnym i archiwach

Projektodawca poprzestał jedynie na stwierdzeniu, że: „do przetwarzania danych osobowych przez jednostki, o których mowa w art. 22, nie stosuje się art. 5 ust. 2 rozporządzenia 2016/679. Taka konstrukcja przepisu mającego wprowadzać w prawie polskim wyjątek od jednej z podstawowych – przewidzianych w rozporządzeniu unijnym – zasad przetwarzania danych osobowych (zasady rozliczalności) nie może zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych, gdyż brak jest wskazania w komentowanym przepisie, względ na którą z wymienionych w art. 23 ust. 1 rozporządzenia unijnego wartości przemawia za wprowadzeniem proponowanego ograniczenia. Podnieść też wypada, iż art. 23 ust. 1 rozporządzenia zakłada możliwość jedynie ograniczenia zakresu niektórych obowiązków i praw z rozporządzenia unijnego, jednakże nie przewiduje całkowitego uchylenia tych praw i obowiązków w prawie państwa członkowskiego (szersze wyłączenie w przypadku przetwarzania danych osobowych do celów archiwalnych w interesie publicznym zawiera art. 89 ust. 3 rozporządzenia), jak ma to miejsce w art. 22c ust. 3 ustawy o narodowym zasobie archiwalnym i archiwach.

Proponowany art. 22c ust. 4 zmienianej ustawy stanowi niedopuszczalne powtórzenie art. 14 ust. 5 lit. b rozporządzenia unijnego oraz art. 17 ust. 3 lit. d rozporządzenia 2016/679 i powinien zostać usunięty.

Kolejna wątpliwość Generalnego Inspektora Ochrony Danych Osobowych dotyczy art. 22c ust. 5 ustawy zgodnie, z którym nie stosuje się art. 34 rozporządzenia, jeżeli jednostka prowadząca działalność archiwalną w zakresie państwowego zasobu archiwalnego w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej. O terminie 72 godzin mówi motyw 85 rozporządzenia, jednakże odnosi się on do zgłaszania takiego naruszenia organowi nadzorczemu (ma to nastąpić bez zbędnej zwłoki, jeżeli to wykonalne, a nie później niż w terminie 72 godzin po stwierdzeniu naruszenia). Natomiast motyw 86 rozporządzenia unijnego stanowi, że administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych. W świetle zaś art. 34 ust. 1 rozporządzenia 2016/679 powyższe zawiadomienie osoby, której dane dotyczą, jest zasadą, od której wyjątkiem – przewidzianym w art. 34 ust. 3 lit. c rozporządzenia – jest możliwość zastąpienia takiego zawiadomienia publicznym komunikatem lub podobnym środkiem, gdy indywidualne zawiadomienie wymaga niewspółmiernie dużego wysiłku. W związku z tym zasadnym jest przeredagowanie zaproponowanego brzmienia art. 22c ust. 5 ustawy o narodowym zasobie archiwalnym i archiwach, albowiem przepis ten, bez spełnienia

żadnych dodatkowych przesłanek, a więc wbrew art. 34 rozporządzenia, jako zasadę przyjmuje zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych poprzez komunikat na stronie podmiotowej w Biuletynie Informacji Publicznej lub stronie internetowej. Pamiętać należy, iż zgłaszanie naruszenia osobom, których dane dotyczą, w myśl art. 34 rozporządzenia następuje wyłącznie w przypadku takich naruszeń, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. A zatem obowiązek zawiadamiania osób, których dane dotyczą, nie dotyczy wszelkich naruszeń ochrony danych osobowych. Przepis rozporządzenia 2016/679 (art. 34) ma charakter gwarancyjny, ma stanowić realne zabezpieczenie praw osoby, której dane dotyczą, umożliwiając szybką reakcję tej osoby w przypadku zaistnienia naruszenia.

#### **19. Zmiana ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2016 r. poz. 1440 z późn. zm.)**

W art. 14 projektu ustawy zaproponowano szeroki katalog danych osobowych w opinii projektodawcy niezbędny do poboru opłaty parkingowej. Należy zwrócić uwagę, iż egzekucja obowiązku została wskazana jedynie w uzasadnieniu. Z obecnego brzmienia propozycji wynika możliwość żądania wszystkich wymienionych danych w celu poboru opłaty. Uznać to należy za zbędne z uwagi na zasady wnoszenia opłat. Ma to miejsce przede wszystkim poprzez uiszczenie jej w kasie i udowodnienie tego faktu poprzez wyłożenie biletu parkingowego w miejscu widocznym w pojeździe. Dopiero w przypadku braku takiej opłaty możliwe powinno być przetwarzanie informacji ujętych w 13fa ust. 2 pkt 1-5 i to rozróżnienie celów w stosunku do zakresów przetwarzanych danych powinno wyraźnie wynikać z przepisów prawa. W zakresie obrazu pojazdu (ust. 2 pkt 5), nie jest jasnym do jakiego celu niezbędny jest wizerunek osób. Konieczne jest w tym zakresie dostosowanie proponowanego przepisu do zasady minimalizacji danych wyrażonej w art. 5 ust. 1 lit. c rozporządzenia 2016/679.

W art. 13hd ust. 3a ustawy użyto dotychczas stosowanej konstrukcji dającej operatorowi możliwość przetwarzania danych. Natomiast zgodnie z art. 6 ust. 1 lit. c rozporządzenia 2016/679 podstawą do przetwarzania może być jedynie obowiązek prawny ciążyący na administratorze. Obecna konstrukcja realizacji uprawnienia albo obowiązku wyrażona w art. 23 ust. 1 lit. b ustawy o ochronie danych osobowych nie będzie po 25 maja przyszłego roku dopuszczalna. Dlatego też konieczna jest zmiana brzmienia przepisu. Analogiczną uwagę należy zgłosić do nowej treści art. 17 ust. 3, 18 ust. 2a, 20h ust. 1 i 2 zmienianej ustawy.

W art. 16i ust. 1 pkt 4 Generalny Inspektor sugeruje doprecyzować, iż porozumienie o współpracy z podmiotem uprawnionym do kontroli prawidłowości uiszczenia opłaty elektronicznej powinno być zgodne z przepisami o ochronie danych – w szczególności w zakresie udostępniania informacji wyłącznie w zakresie niezbędnym do prowadzenia w/w kontroli.

Odnosząc się do ust. 1a projektodawca powinien zweryfikować, jakie dane identyfikacyjne są niezbędne. W przypadku przetwarzania Numeru Informacji Podatkowej, zbędnym powinno być przetwarzanie rodzaju, serii i numeru dokumentu tożsamości.

W art. 17 ust. 3 oraz 4 pkt 2 należy zweryfikować zakres odesłań do art. 24n ust. 5 i 7. O ile w ust. 7 mowa jest o zadaniu ministra polegającym na przedłużeniu obowiązywania certyfikatu, to ust. 5 reguluje obowiązek uczelni dot. prowadzenia określonego kierunku zajęć. Nie jest to zadanie ministra wł. ds. transportu. Co do zakresu danych należy poddać w wątpliwość konieczność przetwarzania daty i miejsca urodzenia, imion ojca i matki oraz nazwiska rodowego matki w obliczu przetwarzania także numeru PESEL, który w sposób wystarczający służy do identyfikacji osoby fizycznej. W związku z treścią uzasadnienia (s. 16) katalog danych należy rozszerzyć o dwie następujące kategorie: dane osobowe o skazaniu, o którym mowa w art. 24n ust. 2 pkt 3 oraz wykształceniu, o którym mowa w art. 24n ust. 2 pkt 4.

W art. 18 ust. 2b sugeruje się doprecyzowanie, iż przetwarzanie rodzaju, serii i numeru dokumentu tożsamości powinno być stosowane wobec osób nie posiadających numeru PESEL albo NIP. Zgodnie z obecnym brzmieniem może dochodzić do przetwarzania danych nadmiernych, co byłoby niezgodne z zasadą minimalizacji danych ujętą w art. 5 ust. 1 lit. c rozporządzenia 2016/679. Projektodawca powinien także wyjaśnić, czy dane korzystającego z autostrady i drogi krajowej (ust. 2b pkt 1 lit. a oraz pkt 2 lit. a) będą zbierane uprzednio, czy po stwierdzeniu nieuiszczenia opłaty. Z uzasadnienia (s. 18) wynika jedynie, iż mają one służyć do wystawiania wezwań do zapłaty.

W odniesieniu do okresu przechowywania danych zaproponowanego w art. 18 ust. 2c projektodawca powinien wyjaśnić, czy będzie to dotyczyło wszystkich użytkowników dróg, którzy będą poddawani kontroli realizacji obowiązku wniesienia opłat za przejazd, czy tylko osób uchylających się od takiej opłaty oraz osób kierujących pojazdami, które niszczą drogi.

Odnosnie realizacji obowiązku informacyjnego (art. 18 ust. 2d) i udostępniania danych osobowych służbom porządkowym oraz specjalnym (art. 18 ust. 2e-2j) aktualne pozostają

stanowiska organu ds. ochrony danych osobowych wyrażone w toku konsultacji z Ministerstwem Finansów<sup>6</sup>.

Powyższe uwagi należy zastosować analogicznie do przepisów art. 20h.

## **20. Zmiana ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2017 r. poz. 958)**

Generalny Inspektor zwraca uwagę, że przewidziane w art. 15 projektowanej ustawy brzmienie art. 17c ustawy o Rzeczniku Praw Obywatelskich budzi wątpliwości z uwagi na zastosowanie wyrażenia „może przetwarzać wszelkie informacje” (ust. 1) oraz „może przetwarzać dane osobowe”. Z punktu widzenia zgodności z wynikającą z art. 51 ust. 2 Konstytucji zasadą adekwatności pozyskiwania, gromadzenia i udostępniania informacji o obywatelach oraz wyrażonej w art. 5 ust. 1 lit. c rozporządzenia 2016/679 zasadą minimalizacji danych właściwszym byłoby posłużenie się bardziej jednoznacznym wyrażeniem wskazującym, że Rzecznik przetwarza informacje oraz przetwarza określone dane, zamiast proponowanego „może przetwarzać”.

## **21. Zmiana ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2016 r. poz. 1943, z późn. zm.)**

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi pozostawienie w art. 95b ust. 1 ustawy o systemie oświaty otwartego katalogu przetwarzanych danych osobowych poprzez użycie sformułowania „w szczególności”. Zgodnie z zasadą minimalizacji danych – art. 5 ust. 1 lit. c rozporządzenia 2016/679 – projektodawca powinien ustanowić zamknięty katalog przetwarzanych danych, adekwatny i ograniczony jedynie do danych niezbędnych do celów, w których są one przetwarzane.

Odnosząc się do art. 95b ust. 3 ustawy o systemie oświaty – w opinii Generalnego Inspektora zachodzi potrzeba przeprowadzenia przez projektodawcę gruntownej analizy zasadności i zakresu, zawnioskowanego w art. 95b ust. 3 ustawy wyłączenia stosowania art. 13 i art. 14 oraz art. 17–19 rozporządzenia 3026/679. Z brzmienia komentowanego przepisu nie wynika bowiem cel zastosowania przedmiotowego wyłączenia ani przyczyna, dla której zostało ono zaproponowane. Przypomnieć zaś wypada, iż prawodawca unijny umożliwił wprowadzenie ograniczeń niektórych praw i obowiązków przewidzianych w rozporządzeniu 2016/679 wyłącznie w przypadku, gdy proponujący takie ograniczenie wykaże, że jest ono niezbędne i proporcjonalne w

---

<sup>6</sup> Sygn. DOLiS-023-237/17/KK/46501 z 7 czerwca 2017 r., DOLiS-023-237/17/KK/56240 z 17 lipca 2017 r., <http://giodo.gov.pl/pl/1520275/10119>, sygn. DOLiS-023-407/17/KK/68668,68675,68676 z 13 września 2017 r.,

demokratycznym społeczeństwie ze względu na wartości wskazane w art. 23 ust. 1 rozporządzenia 2016/679. Tymczasem w art. 95b ust. 3 ustawy poprzestano jedynie na autorytatywnym stwierdzeniu, iż: „art. 13 i art. 14 oraz art. 17–19 rozporządzenia 2016/679 nie stosuje się”, nie odnosząc się w żaden sposób do – wyżej zaprezentowanych – kwestii podniesionych w art. 23 ust. 1 rozporządzenia.

Art. 95b ust. 4 ustawy o systemie oświaty - Kształt tego wyłączenia wymaga ponownej weryfikacji i ewentualnego dalszego doprecyzowania w świetle argumentów przedstawionych w uwadze do art. 22c ust. 3 ustawy o narodowym zasobie archiwalnym i archiwach.

Przepis art. 95b ust. 5 ustawy o systemie oświaty, zgodnie z którym nie stosuje się art. 34 rozporządzenia unijnego, jeżeli administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej, wymaga poprawienia.

O terminie 72 godzin mówi motyw 85 rozporządzenia 2016/679, jednakże odnosi się on do zgłaszania takiego naruszenia organowi nadzorczemu (ma to nastąpić bez zbędnej zwłoki, jeżeli to wykonalne, a nie później niż w terminie 72 godzin po stwierdzeniu naruszenia). Natomiast motyw 86 rozporządzenia 2016/679 stanowi, że administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych. W świetle zaś art. 34 ust. 1 rozporządzenia 2016/679 powyższe zawiadomienie osoby, której dane dotyczą, jest zasadą, od której wyjątkiem – przewidzianym w art. 34 ust. 3 lit. c rozporządzenia 2016/679 – jest możliwość zastąpienia takiego zawiadomienia publicznym komunikatem lub podobnym środkiem, gdy indywidualne zawiadomienie wymaga niewspółmiernie dużego wysiłku. W związku z tym zasadnym jest preredagowanie zaproponowanego brzmienia art. 95b ust. 5 ustawy o systemie oświaty, albowiem przepis ten, bez spełnienia żadnych dodatkowych przesłanek, a więc wbrew art. 34 rozporządzenia 2016/679, jako zasadę przyjmuje zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych poprzez komunikat na stronie podmiotowej w Biuletynie Informacji Publicznej lub stronie internetowej. Pamiętać należy, iż zgłaszanie naruszenia osobom, których dane dotyczą, w myśl art. 34 rozporządzenia unijnego następuje wyłącznie w przypadku takich naruszeń, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. A zatem obowiązek zawiadamiania osób, których dane dotyczą, nie dotyczy



wszelkich naruszeń ochrony danych osobowych. Przepis rozporządzenia 2016/679 (art. 34) ma charakter gwarancyjny, ma stanowić realne zabezpieczenie praw osoby, której dane dotyczą, umożliwiając szybką reakcję tej osoby w przypadku zaistnienia naruszenia.

Przepis art. 95b ust. 6 ustawy ten wymaga ponownego zweryfikowania przez projektodawcę co do jego merytorycznej prawidłowości i zgodności z rozporządzeniem unijnym.

## **21. Zmiany w z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz. U. z 2017 r. poz. 862)**

W art. 19 projektu koniecznym jest doprecyzowanie w przepisach ustawy o działalności kulturalnej, celu, w jakim będą przetwarzane dane osobowe określone w:

- 1) dodawanym do art. 6a ust. 2a ustawy, określającym zakres danych osobowych, które będzie przetwarzał Minister Kultury i Dziedzictwa Narodowego kandydata i odznaczonego do odznaki honorowej „Zasłużony dla kultury polskiej”,
- 2) dodawanym do art. 7 ust. 4a, określającym zakres danych przetwarzanych przez Ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego kandydata lub odznaczonego na medal „Zasłużony Kulturze Gloria Artis” (zasada minimalizmu, proporcjonalności).

Powinny one być zgodne z zasadą minimalizacji danych ujętą w art. 5 ust. 1 lit. c RODO.

W opinii Generalnego Inspektora wyjaśnienia wymaga proponowany okres przechowywania danych osobowych gromadzonych w związku z nadaniem odznaki honorowej „Zasłużony dla Kultury Polskiej” oraz z nadaniem Medalu „Zasłużony Kulturze Gloria Artis”, który zgodnie z dodawanym do art. 6 a ust. 2 b oraz dodawanym do art. 7 ust. 4b ma wynosić 80 lat. W tym samym zakresie należałoby wyjaśnić zaproponowany 5-letni okres przechowywania danych osobowych gromadzonych w związku z przyznaniem nagrody za osiągnięcia w dziedzinie twórczości artystycznej, upowszechniania i ochrony kultury lub stypendium osobom zajmującym się twórczością artystyczną, upowszechnianiem kultury oraz opieką nad zabytkami (art. 7a ust. 2b).

Wyjaśnienia wymaga zasadność pozyskiwania numeru PESEL od kandydatów lub nagrodzonych (w art. 7a ust. 2a) jak i wnioskodawcy lub stypendysty (w art. 7 b ust. 2). Zwrócić również należy uwagę, iż pozyskiwanie numeru telefonu oraz adresu poczty elektronicznej nie może być obowiązkowe, lecz dobrowolne (art. 7a ust. 2a, art. 7b ust. 2a, art. 16b, art. 37 e ust.1).

Na podstawie dodawanego do art. 7 b ust. 2a pkt 11 podmiot przyznający stypendium będzie przetwarzał dane związane z sytuacją życiową wnioskodawcy lub stypendysty. Zgodnie zaś z ust. 2b dodawanym do tego artykułu dane o stanie zdrowia stypendysty, przekazane przez

stypendystę na podstawie ust. 2 a pkt 11, nie podlegają dalszemu udostępnianiu. Kwestia ta powinna zostać przez projektodawcę wyjaśniona.

Należy pamiętać, iż nie tylko dane o stanie zdrowia stypendysty stanowią szczególne kategorie danych w rozumieniu art. 9 rozporządzenia 2016/679. W pojęciu „dane związane z sytuacją życiową” mogą się mieścić także dane dotyczące zdrowia w rozumieniu art. 4 pkt 15 rozporządzenia 2016/679 innych osób itp. W związku z powyższym wszystkie dane osobowe związane z sytuacją życiową o których mowa w art. 7b ust. 2a pkt 11 powinny znajdować się pod szczególną ochroną wynikającą z przepisów prawa a przepisy prawa powinny zagwarantować to poprzez właściwe regulacje. Nie wydaje się także zasadnym przechowywanie tych danych przez okres 5 lat (ust. 2c).

W dodawanym art. 16 b doprecyzowania wymaga czyje dane osobowe będą przetwarzane w związku z powoływaniem i odwoływaniem dyrektora instytucji kultury etc. (np. kandydatów na stanowisko).

W opinii Generalnego Inspektora Ochrony Danych Osobowych dodawany do ustawy art. 37 e jest zbyt ogólny. Przepis ten daje bowiem możliwość przetwarzania danych osobowych nieskonkretyzowanych osób, w bardzo szerokim zakresie, przez szereg podmiotów w celach bardzo szeroko ujętych (realizacja zadań o których mowa w art. 1 ust. 1-4, art. 5, art. 9 ust.3 oraz art. 28 ust. 1a i 1b). Konstrukcja tego przepisu pozwala na bardzo szeroką interpretację, co może prowadzić do pozyskiwania danych osobowych w szerszym zakresie, niż jest to niezbędne przez wskazane w przepisie podmioty. Należy zatem przepis ten sprecyzować poprzez wskazanie – w jakim zakresie, przez jakie podmioty i w jakim konkretnie celu – do realizacji jakich konkretnie zadań dane osobowe będą przetwarzane.

W art. 37 e ust. 2 należałoby doprecyzować – w jakich sytuacjach, w jakich celach - czy w celu realizacji wspólnego przedsięwzięcia etc. ma dochodzić do powierzania przetwarzania danych osobowych pomiędzy podmiotami wykonującymi zadania z zakresu działalności kulturalnej. Generalny Inspektor Ochrony Danych Osobowych uwagę w zakresie konstrukcji przepisów dotyczących powierzenia danych ujął w opinii do art. 21 projektu.

## **22. Zmiany w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2017 r. poz. 880 i 1089)**

Odnosząc się do art. 21 projektu Generalny Inspektor z aprobatą przyjmuje rozwiązanie legislacyjne zawarte w art. 35<sup>2</sup> ust. 1 ustawy o prawie autorskim i prawach pokrewnych polegające na przeniesieniu do projektowanego przepisu katalogu danych przetwarzanych w pisemnym oświadczeniu o woli otrzymywania wynagrodzenia z rozporządzenia wykonawczego, które

skutkuje uchYLENIEM art. 35<sup>4</sup> pkt 3 ustawy (obecna delegacja ustawowa dookreślająca katalog danych wymaganych w oświadczeniu).

W odniesieniu do Rozdziału 13<sup>1</sup> Ochrona Danych Osobowych zmienianej ustawy Generalny Inspektor zgłasza następujące uwagi.

Wątpliwości Generalnego Inspektora budzi pozostawianie otwartego katalogu przetwarzania danych osobowych w art. 114a ust. 1-3 poprzez użycie słowa „w szczególności”. Zgodnie z zasadą minimalizacji danych projektodawca powinien ustanowić zamknięty katalog przetwarzanych danych, adekwatny i ograniczony jedynie do zakresu danych niezbędnych do realizacji celów, dla których dane te są przetwarzane. Jednocześnie w przypadku przetwarzania danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych – mając na uwadze, że w polskim porządku prawnym nie istnieje obowiązek posiadania przez osoby fizyczne takich środków komunikacji – należy pozostawić swobodę możliwości podawania takich danych. Dodatkowo zdaniem organu ds. ochrony danych osobowych, pozyskiwanie danych o imionach rodziców danej osoby, dacie i miejscu jej urodzenia jest nadmiarowe. Dane osobowe wymienione w każdym z ustępów art. 114a ustawy o prawie autorskim i prawach pokrewnych takie jak imię i nazwisko, adres zamieszkania lub do korespondencji, wykształcenie, miejsce pracy i zajmowane stanowisko są wystarczające do identyfikacji danej osoby.

Projektodawca przepisem art. 114b ust. 1 ustawy o prawie autorskim i prawach pokrewnych ogranicza stosowanie art. 12 i 15 rozporządzenia 2016/679 w stosunku do przetwarzania danych osobowych, o których mowa w art. 114a poprzez wskazanie, że prawa te są realizowane raz na 6 miesięcy bezpłatnie, w innych przypadkach odpłatnie. Nie jest jasna przyczyna przedmiotowego ograniczenia choć w uzasadnieniu do projektowanych rozwiązań wskazuje się, że jest ono uzasadnione interesem finansowym państwa cyt. „minister właściwy do spraw kultury i dziedzictwa narodowego oraz organizacja zbiorowego zarządzania jako podmioty publiczne narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń”. Jeżeli zatem projektodawca widzi potrzebę ograniczenia stosowania art. 12 i 15 rozporządzenia 2016/679 poprzez zastosowanie wyłączenia z art. 23 ust. 1 lit. e rozporządzenia 2016/679, to powinien nie tylko jasno wskazać przyczynę wyłączenia w przepisie art. 114b ust. 1 ustawy o prawie autorskim i prawach pokrewnych lecz również spełnić warunki, którym powinien odpowiadać akt prawny zawierający takie wyłączenia z art. 23 ust. 2 lit. a – h RODO. **Podobną uwagę Generalny Inspektor kieruje do art. 114b ust. 2**, zgodnie z którym do przetwarzania danych osobowych, o których mowa w art. 114a ustawy o prawie autorskim i prawach pokrewnych, przepisów art. 14 rozporządzenia

2016/679 nie stosuje się w zakresie, w jakim dane te są niezbędne do zapewnienia prawidłowej realizacji zadań, o których mowa w art. 20, 20<sup>1</sup>, art. 28 ust. 4 i 5, art. 35<sup>2</sup>, 35<sup>6</sup>, 35<sup>7</sup>, 35<sup>11</sup>, 110<sup>27</sup> i 110<sup>28</sup> ustawy o prawie autorskim i prawach pokrewnych. Z przepisu nie wynika jednak jaka konkretnie przesłanka z art. 23 ust. 1 lit. a-j rozporządzenia 2016/679 będzie zastosowana w tym przypadku.

Konstrukcją przepisów art. 114a projektodawca częściowo spełnia warunki określone w art. 23 ust. 2 lit. a – h rozporządzenia 2016/679, tj. cele przetwarzania (realizacja zadań), kategorie danych osobowych (wskazuje katalog danych), zakres wprowadzanych ograniczeń (art. 114b ust. 1-3), określa administratorów poprzez wskazanie odpowiednio ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego, organizacji zbiorowego zarządzania prawami autorskimi lub prawami pokrewnymi, podmioty wymienione w art. 35<sup>5</sup> ust. 2 ustawy o prawie autorskim i prawach pokrewnych tj. archiwa, instytucje oświatowe, uczelnie itd. (każde ze zdań w art. 114a ust. 1-3 będące wstępem do wyliczenia), informuje również o ograniczeniach, które ustanawia przepisami art. 114b.

Niemniej jednak, w opinii Generalnego Inspektora doprecyzowania wymaga kwestia retencji danych. Zgodnie z motywem 39 rozporządzenia 2016/679 aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien zapewnić ograniczenia okresu przechowywania danych do ścisłego minimum, czyli ustalić termin ich usuwania lub okresowego przeglądu.

Kolejna wątpliwość Generalnego Inspektora dotyczy treści art. 114b ust. 3, zgodnie z którym nie stosuje się art. 34 rozporządzenia 2016/679, jeżeli administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w BIP lub na swojej stronie internetowej. O terminie 72 godzin mówi motyw 85 rozporządzenia 2016/679, a odnosi się do zgłaszania takiego naruszenia organowi nadzorczemu bez zbędnej zwłoki – jeżeli jest to wykonalne – nie później niż w terminie 72 godzin. Natomiast motyw 86 stanowi, że administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. W związku z powyższym słuszne wydaje się przeredagowanie obecnego brzmienia art. 114b ust. 3 ustawy o prawie autorskim i prawach pokrewnych. Jednocześnie trzeba zauważyć, że zgłaszanie naruszenia osobom, których dane dotyczą, zgodnie z art. 34 rozporządzenia 2016/679 następuje wyłącznie w przypadku wysokiego ryzyka naruszenia praw i wolności, osób których dane dotyczą. W związku z tym, obowiązek powiadamiania tych osób nie

dotyczy wszelkich naruszeń. Co więcej przepis ten ma stanowić realne zabezpieczenie i umożliwić szybką reakcję osoby, której dane dotyczą w przypadku zaistnienia naruszenia. W art. 34 ust 3 rozporządzenia 2016/679 wskazano sytuacje, w jakich zawiadomienie nie jest wymagane. Zatem zastrzeżenia Generalnego Inspektora muszą budzić wszystkie projektowane przepisy dotyczące wyłączenia stosowania art. 34 rozporządzenia 2016/679, tym bardziej że projektodawca wskazuje jedynie interes finansowy państwa jako uzasadnienie dla tego wyłączenia.

Konstrukcja przepisu art. 114b ust. 1 wskazuje, że projektodawca czerpał pewne rozwiązania z art. 12 ust. 5 lub z art. 15 ust. 3 rozporządzenia 2016/679. Wyjaśnić jednak należy, że przepisy te w odniesieniu do pobierania opłat za informacje powinny mieć zastosowanie odpowiednio tylko wtedy, kiedy żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter lub przy wydawaniu kolejnej kopii danych podlegających przetwarzaniu. Generalny Inspektor zwraca uwagę na kwestię indywidualnego podejścia do każdej z rozpatrywanych spraw dotyczących prawa dostępu przysługującego osobie, której dane dotyczą (art. 15 rozporządzenia 2016/679). Oznacza to, że każdy administrator rozpatrując daną sprawę będzie dokonywał oceny danego stanu faktycznego w sposób indywidualny, a nie generalny, a więc proponowane ograniczenie będzie niezgodne z art. 12 ust. 5 i z art. 15 ust. 3 rozporządzenia 2016/679.

**Podsumowując uwagi dotyczące stosowanych w projektowanych przepisach ograniczeń z art. 23 RODO,** należy stwierdzić, że projektodawca opiera się na przede wszystkim na przesłance określającej inne ważne cele leżące w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu. Jednak zgodnie ze stanowiskiem prezentowanym w orzecznictwie NSA<sup>7</sup> względy natury organizacyjno-finansowej nie powinny być traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych. Powyższe stanowisko w pełni zachowuje aktualność, również na gruncie ogólnego rozporządzenia o ochronie danych. A zatem uzasadnienie takie z pewnością nie jest wystarczające.

Kolejną uwagę Generalny Inspektor kieruje do treści art. 114b ust. 5, który dubluje, powiela postanowienia treści art. 23 ust. 2 lit. d rozporządzenia 2016/679. Konieczność prawidłowego zabezpieczenia danych osobowych wynika wprost z przepisów rozporządzenia i obowiązek ten ciąży na każdym administratorze. Nieuzasadnione jest zatem przenoszenie w całości bądź tylko w części ich przepisów. Powodować to może nieprawidłową ich interpretację. W związku z tym

---

<sup>7</sup> Sygn. akt II SA 3144/01

konieczne wydaje się uregulowanie tych kwestii, które zagwarantuje, że każdy z administratorów wykonując swoje ustawowe zadania zapewni bezpieczeństwo przetwarzania danych osobowych podejmując działania mające na celu zapewnienie zgodności przetwarzania z wymogami rozporządzenia 2016/679.

Generalny Inspektor zgłasza uwagę także do art. 114b ust 6, zgodnie z którym minister właściwy do spraw kultury i dziedzictwa narodowego, organizacja zbiorowego zarządzania prawami autorskimi lub prawami pokrewnymi i podmioty wymienione w art. 35<sup>5</sup> ust. 2 (ustawy o prawie autorskim i prawach pokrewnych) mogą zlecać przetwarzanie w ich imieniu danych osobowych lub pełnić funkcje podmiotu przetwarzającego dane osobowe na zlecenie innego podmiotu.

Instytucja powierzenia przetwarzania danych osobowych jest co do zasady dopuszczalna przez rozporządzenie 2016/679 na podstawie art. 28 rozporządzenia. Przepis ten jak i doprecyzowujący go motyw 81 rozporządzenia 2016/679 określają zasady przetwarzania danych osobowych przez podmiot przetwarzający w imieniu administratora. Analiza art. 28 i następnych rozporządzenia 2016/679 wskazuje, że postanowienia projektowanego art. 114b ust. 6 są niewystarczające. Zgodnie z art. 28 ust. 3 przetwarzanie danych osobowych przez podmiot przetwarzający powinno odbywać się na podstawie umowy lub innego instrumentu prawnego (przepisów ustawy), które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Taka umowa lub inny instrument prawny powinny spełniać w szczególności warunki wymienione w art. 28 ust. 3 lit a-h oraz ustępach dalszych. Tego rodzaju ogólna regulacja, stosująca określenia nieostre i niewystępujące w rozporządzeniu 2016/679 takie jak „może zlecać”, bez jednoczesnego stworzenia w tym zakresie odpowiednich gwarancji, w szczególności jasnego określenia zasad, na jakich to powierzenie ma mieć miejsce, jest niewystarczającą podstawą do powierzenia przetwarzania danych.

### **23. Zmiana ustawy z dnia 14 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (Dz. U. z 2016 r., poz. 800, 1984 i 2255)**

Dodany przepis art. 8 ust. 1<sup>1</sup> - 1<sup>4</sup> zmienianej ustawy stanowi, że „w celu uzyskania ulgowej usługi i świadczenia osoba uprawniona wyraża zgodę na podanie jej danych osobowych, danych osobowych członków jej rodziny oraz innych osób pozostających z nią we wspólnym gospodarstwie domowym”. W kolejnym ust. 1<sup>2</sup>, wskazuje się, że „wyrażenie zgody, o której mowa

w ust. 1<sup>1</sup>, następuje w oświadczeniu złożonym w postaci papierowej lub elektronicznej. Zgoda jest wyrażana przy poszanowaniu pełnej swobody w jej udzielaniu.” Powyższy przepis będący klauzulą zgody jest zbędny w projekcie zmiany ustawy z punktu widzenia przepisów ogólnego rozporządzenia. W art. 6 ust. 1 pkt a-f rozporządzenia 2016/679 wskazane zostały przesłanki przetwarzania danych i spełnienie jednej z tych przesłanek jest wystarczające, aby warunek legalności był wypełniony. Jak stanowi art. 6 ust. 1 lit. c ogólnego rozporządzenia, przetwarzanie danych jest zgodne z prawem w przypadku, gdy przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Jeżeli zatem w przepisie prawnym ustanawia się obowiązek udostępnienia pracodawcy w formie oświadczenia danych osobowych pracownika i członków jego rodziny to odpowiada to ww. przesłance, a w konsekwencji nadmiarowe i zbędne jest pozyskiwanie zgody na takie przetwarzanie danych osobowych. Zatem Generalny Inspektor wnioskuję o wykreślenie ust. 1<sup>1</sup> i 1<sup>2</sup> art. 8 zmienianej ustawy. Ponadto należy zwrócić uwagę, że przepisy rozporządzenia 2016/679, poza sytuacją wyrażania zgody za dziecko do lat 16 przez osobę sprawującą władzę rodzicielską lub opiekę, albo za osoby ubezwłasnowolnione, nie przewidują możliwości wyrażenia zgody za osobę trzecią.

Zgodnie z proponowaną zmianą art. 8 ust. 1<sup>1</sup> ustawy o zakładowym funduszu świadczeń socjalnych, osoba uprawniona obowiązana jest podać: imię, nazwisko, datę urodzenia, stopień pokrewieństwa, adres zamieszkania, a także innych danych osobowych tych osób (osób, które pozostają z nią we wspólnym gospodarstwie domowym), jeżeli podanie takich danych jest niezbędne do ustalenia sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej. Generalny Inspektor wskazuje, że podanie daty urodzenia ww. osób jest zasadne wyłącznie w sytuacji, gdy ma wpływ na przyznanie świadczenia, lub określanie jego wysokości. Pozyskiwanie bowiem każdorazowo tej danej osobowej osoby uprawnionej lub osób, które pozostają z nią we wspólnym gospodarstwie powoduje naruszenie zasady minimalizacji danych, uregulowanej w art. 5 ust. 1 pkt c rozporządzenia.

Jeżeli projektodawca przewidział zgodę na podanie danych osobowych osoby korzystającej ze świadczeń socjalnych, jak również członków rodziny to odnotować należy problem realizacji prawa do wycofania tej zgody w każdym momencie, wynikające z art. 7 ust. 3 rozporządzenia 2016/679.

Ponadto należy zwrócić uwagę, że przepisy rozporządzenia, poza sytuacją wyrażania zgody za dziecko do lat 16 przez osobę sprawującą władzę rodzicielską lub opiekę, albo za osoby ubezwłasnowolnione, nie przewidują możliwości wyrażenia zgody za osobę trzecią.

Zatem Generalny Inspektor wnioskuje o wykreślenie ust. 1<sup>1</sup> i 1<sup>2</sup> art. 8 projektu zmiany ustawy.

Jednocześnie należy zwrócić uwagę, iż projektodawca regulując obowiązek wyrażenia zgody przez osobę, która chce korzystać ze świadczeń socjalnych na podanie jej danych i danych członków rodziny pracodawcy nie wskazuje w jaki sposób (w jakiej formie) mają zostać udokumentowane dane dotyczące sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej. Zgodnie z proponowaną zmianą – dodawanym art. 8 ust. 1<sup>1</sup> - ustawy o zakładowym funduszu świadczeń socjalnych, osoba uprawniona obowiązana jest podać: imię, nazwisko, datę urodzenia, stopień pokrewieństwa, adres zamieszkania, a także inne dane osobowe tych osób (osób, które pozostają z nią we wspólnym gospodarstwie domowym), jeżeli podanie takich danych jest niezbędne do ustalenia sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej. Generalny Inspektor wskazuje, że podanie daty urodzenia ww. osób jest zasadne wyłącznie w sytuacji, gdy ma wpływ na przyznanie świadczenia, lub określanie jego wysokości. Pozyskiwanie bowiem każdorazowo tej danej osobowej osoby uprawnionej lub osób, które pozostają z nią we wspólnym gospodarstwie powoduje naruszenie zasady minimalizacji danych, uregulowanej w art. 5 ust. 1 pkt c ogólnego rozporządzenia.

#### **24. Zmiana ustawy z dnia 27 października 1994 r. o autostradach płatnych oraz o Krajowym Funduszu Drogowym (Dz. U. z 2015 r. poz. 641 i 2260)**

W art. 25 projektu użyto dotychczas stosowanej konstrukcji dającej Generalnemu Dyrektorowi Dróg Krajowych i Autostrad możliwość przetwarzania danych. Natomiast zgodnie z art. 6 ust. 1 lit. c RODO podstawą do przetwarzania może być jedynie obowiązek prawny ciążyący na administratorze. Obecna konstrukcja realizacji uprawnienia albo obowiązku wyrażona w art. 23 ust. 1 lit. b ustawy o ochronie danych osobowych nie będzie po 25 maja przyszłego roku dopuszczalna. Dlatego też konieczna jest zmiana brzmienia przepisu.

#### **25. Zmiana ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524, z późn. zm.)**

W związku z wprowadzeniem w art. 9 ust. 1 rozporządzenia 2016/679 szczególnych kategorii danych osobowych, różniących się, tak pod względem katalogu, jak i zakresu poszczególnych pojęć użytych w tym przepisie, od uregulowań dotyczących danych szczególnie chronionych z art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), zachodzi potrzeba odpowiedniego dostosowania brzmienia art. 29 ust. 1 pkt 2



lit. i ustawy o Najwyższej Izbie Kontroli, uwzględniającego powyższe odmienności. Należy przy tym wziąć pod uwagę rozszerzenie w art. 9 ust. 1 rozporządzenia 2016/679 katalogu szczególnych kategorii danych osobowych w stosunku do listy danych szczególnie chronionych z art. 27 ust. 1 ustawy o ochronie danych osobowych.

## **26. Zmiana ustawy z dnia 5 stycznia 1995 r. o fundacji - Zakład Narodowy imienia Ossolińskich (Dz. U. z 2017 r. poz. 1881)**

W ramach art. 27 projektu wątpliwości Generalnego Inspektora budzi przetwarzanie danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych (art. 5 ust. 2 pkt 8 i art. 15 ust. 2a pkt 3 ustawy o fundacji Zakład Narodowy imienia Ossolińskich) oraz imion rodziców danej osoby, daty i miejsca jej urodzenia (art. 5 ust. 2 tej ustawy) co wskazane zostało już w argumentacji do art. 21 projektu.

Podobną uwagę jak do art. 5 ust. 2 pkt 8 rozporządzenia 2016/679 zgłasza do art. 15 ust 2a pkt 3 w przypadku pozyskiwania numeru telefonu i adresu poczty elektronicznej. Jeżeli będą to dane związane z wykonywaniem pracy, zadań służbowych to należy dookreślić ich charakter poprzez dodanie wyrażenia „służbowy/a”.

W odniesieniu do art. 17a ust. 1 ustawy o fundacji Zakład Narodowy imienia Ossolińskich Generalny Inspektor wskazuje, że przepis ten powiela postanowienia treści art. 23 ust. 2 lit. d rozporządzenia 2016/679, a zatem aktualne w tym zakresie pozostają uwagi do art. 21 projektu ustawy - Przepisy wprowadzające. Przepisem art. 17a ust. 2 ustawy o fundacji Zakład Narodowy imienia Ossolińskich ogranicza się stosowanie art. 12 i 15 rozporządzenia 2016/679 wobec przetwarzania danych osobowych, o których mowa w art. 5 ust. 2, art. 12 ust. 2a i art. 15 ust 2a ustawy o fundacji Zakład Narodowy imienia Ossolińskich. W kwestii wyłączeń i ograniczeń stosowania rozporządzenia 2016/679 aktualna pozostaje argumentacja wskazana w art. 21 projektu. Art. 17a ust. 3 stanowi, że do przetwarzania danych osobowych, o których mowa w art. 5 ust. 2, art. 12 ust. 2a i art. 15 ust. 2a, nie stosuje się art. 5 ust. 2 rozporządzenia 2016/679, w zakresie obowiązku wykazywania przestrzegania przepisów art. 5 ust. 1 tego rozporządzenia oraz art. 13-14 i art. 17-19 rozporządzenia, w zakresie, w jakim dane te są niezbędne do zapewnienia prawidłowej realizacji celów i zadań, o których mowa w art. 5 ust. 1, art. 12 ust. 1 i art. 15 ust. 2. Ministerstwo argumentuje ograniczenie interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego oraz Zakład jako podmioty publiczne narażone byłby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w

powyższych przepisach bez ograniczeń. Również w kwestii powyższych ograniczeń i wyłączeń argumentacja Generalnego Inspektora wskazana w art. 2 i 21 pozostaje aktualna.

Przepis art. 17a ust. 4 reguluje wyłączenie stosowania art. 34 rozporządzenia 2016/679 w przypadku gdy odpowiedni zakład albo minister właściwy do spraw kultury i ochrony dziedzictwa narodowego w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej Biuletynu Informacji Publicznej lub na swojej stronie internetowej. Aktualna w tej kwestii pozostaje argumentacja przedstawiona w uwagach do art. 21 projektu ustawy.

Art. 17a ust. 6 przewiduje, że zakład oraz minister właściwy do spraw kultury i ochrony dziedzictwa narodowego mogą zlecać przetwarzanie w swoim imieniu danych osobowych lub pełnić funkcję podmiotu przetwarzającego dane osobowe na zlecenie innego podmiotu. Jest to konstrukcja zlecania przetwarzania podobna do użytej już w ustawie zmienianej w art. 21 zatem nieprawidłowość zastosowania takiej konstrukcji prawnej opisywana była już w art. 21 projektu

## **27. Zmiana ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2016 r. poz. 1068, z późn. zm.)**

Generalny Inspektor Ochrony Danych Osobowych jest zobligowany do zgłoszenia zasadniczego sprzeciwu wobec znacznej części –zaproponowanych w art. 28 projektu zmian ustawy o statystyce publicznej.

Przypomnieć wypada, iż aktualne brzmienie ustawy o statystyce publicznej zostało wypracowane w wyniku wszechstronnych, wyczerpujących, niekiedy wieloletnich uzgodnień między służbami statystyki publicznej (w tym zwłaszcza Prezesem Głównego Urzędu Statystycznego) a Generalnym Inspektorem Ochrony Danych Osobowych. Tymczasem niektóre z przedłożonych do zaopiniowania unormowań ustawy o statystyce publicznej, zamieszczonych w art. 28 projektu, oznaczają całkowite odejście od poczynionych ustaleń. Zaproponowane zmiany w ustawie o statystyce publicznej zawarte w art. 28 projektu ustawy mają bardzo szeroki zakres, który nie powinien być procedowany w ramach ustawy- przepisy wprowadzające ustawę o ochronie danych osobowych. Zakres wprowadzanych zmian należałoby również przeanalizować pod kątem § 84 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz. U. z 2016 r. poz. 283), który stanowi, że jeżeli zmiany wprowadzane w ustawie miałyby być liczne albo miałyby naruszać konstrukcję lub spójność ustawy albo gdy ustawa była już poprzednio wielokrotnie nowelizowana, opracowuje się projekt nowej ustawy.”.

Niedopuszczalne jest więc „przemycanie” w projekcie ustawy wprowadzającej, mającej na celu umożliwienie stosowania w polskim porządku prawnym rozporządzenia 2016/679, rozwiązań ustawy o statystyce publicznej, które nie pozostają w związku z tym rozporządzeniem, lecz zmieniają model funkcjonowania statystyki publicznej.

Tak gruntowne zmiany przepisów o statystyce publicznej wymagają opracowania projektu nowej ustawy o statystyce publicznej, który będzie podlegał procesowi opiniowania i uzgadniania z zainteresowanymi podmiotami, a nie „zniknie” w procedurze uzgodnień wielkiego (liczącego ponad 170 stron i nowelizującego ponad 130 ustaw) projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych.

Mając na uwadze powyższe wskazać trzeba, że:

- a) nowe brzmienie art. 5 ust. 3 ustawy o statystyce publicznej, które ma być wprowadzone przez art. 28 pkt 3 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych, wyłącza przy przekazywaniu danych do celów statystycznych stosowanie ograniczeń wynikających z obowiązku zachowania tajemnic ustawowo chronionych, z wyjątkiem ograniczeń wynikających z konieczności ochrony informacji niejawnych (odmiennie obowiązujący art. 5 ust. 2 ustawy o statystyce publicznej),
- b) uchylenie art. 9 ust. 1 ustawy o statystyce publicznej – art. 28 pkt 8 lit. a projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych – oznacza zniesienie, istniejącego od ponad 30 lat, obowiązku wydawania odrębnej ustawy dla przeprowadzenia spisu powszechnego, w ramach którego osoby fizyczne są zobowiązane do udzielania informacji służbom statystyki publicznej,
- c) ulega poważnemu rozszerzeniu katalog danych, do przetwarzania których służby statystyki publicznej są uprawnione i to m.in. o dane szczególnych kategorii takie jak: dane biometryczne, dane genetyczne, dane dotyczące seksualności i informacje o pozostawaniu w konkubinacie – art. 35b ust. 1 pkt 5a–5c ustawy o statystyce publicznej, które mają być dodane przez art. 28 pkt 18 lit. a tiret czwarte projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych oraz art. 35b ust. 1 pkt 12a ustawy o statystyce publicznej, który ma być dodany przez art. 28 pkt 18 lit. a tiret piąte projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych,
- d) zmieniony zostaje, i to znacznie, zakres dziedzin, w których badania statystyczne mogą być prowadzone – art. 35b ust. 2 ustawy o statystyce publicznej, w brzmieniu nadanym

przez art. 28 pkt 18 lit. b projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych,

- e) ma być uchylony, przewidziany w obowiązującym art. 35d ustawy o statystyce publicznej, wymóg usunięcia, zebranych przez służby statystyki publicznej, danych umożliwiających identyfikację osób fizycznych najpóźniej po upływie 10 lat od zebrania tych danych – nowe brzmienie art. 35d ustawy o statystyce publicznej, które ma być wprowadzone przez art. 28 pkt 20 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych,
- f) uchylenie art. 35e ustawy o statystyce publicznej –art. 28 pkt 21 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych – oznacza zniesienie zakazu gromadzenia w jednym zbiorze danych wszystkich zebranych przez służby statystyki publicznej danych dotyczących konkretnej osoby fizycznej, które w połączeniu mogłyby służyć do charakterystyki lub oceny tej osoby,
- g) całkowitej zmianie podlegają przepisy odnoszące się do prowadzenia przez Prezesa Głównego Urzędu Statystycznego operatu do badań statystycznych – art. 39a–39c ustawy o statystyce publicznej, które mają być dodane przez art. 28 pkt 25 projektu ustawy –Przepisy wprowadzające ustawę o ochronie danych osobowych.

Przechodząc do zmienianych przepisów ustawy o statystyce publicznej, które mają rzeczywisty związek z kwestią stosowania w polskim porządku prawnym rozporządzenia 2016/679, Generalny Inspektor Ochrony Danych Osobowych oponuje przeciwko dyspozycji art. 35h ust. 2 pkt 1 ustawy o statystyce publicznej, który ma być dodany przez art. 28 pkt 23 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych. Choć prawodawca unijny w art. 23 ust. 1 rozporządzenia 2016/679 dopuścił m.in. ograniczenie stosowania zasady rozliczalności z art. 5 ust. 2 rozporządzenia unijnego, obwarował wprowadzenie takiego ograniczenia określonymi wymogami, które należy wykazać. Tymczasem w kwestionowanym art. 35h ust. 2 pkt 1 zmienianej ustawy projektodawca poprzestał na lakonicznym sformułowaniu, że – będąca w rozporządzeniu unijnym jedną z podstawowych zasad przetwarzania danych osobowych – zasada rozliczalności podlega ograniczeniu, gdy [...] realizacja spowodowałaby nadmierny koszt po stronie służb statystyki publicznej. Taka konstrukcja przepisu mającego wprowadzać w prawie polskim wyjątek od zasad przetwarzania danych osobowych przewidzianych w rozporządzeniu 2016/679 nie może zyskać akceptacji Generalnego Inspektora, albowiem brak jest w nim wskazania, która z

wymienionych w art. 23 ust. 1 rozporządzenia 2016/679 wartości przemawia za wprowadzeniem proponowanego ograniczenia i – co więcej – jaki miałby być jego zakres. Podnieść również wypada, że art. 23 ust. 1 rozporządzenia 2016/679 zakłada możliwość ograniczenia zakresu niektórych obowiązków i praw z rozporządzenia 2016/679, jednakże nie przewiduje całkowitego uchylenia tych praw i obowiązków w prawie państwa członkowskiego (szersze wyłączenie w przypadku przetwarzania danych osobowych do celów statystycznych zawiera art. 89 ust. 2 rozporządzenia).

Podobną uwagę do powyższej zgłosić należy do art. 35h ust. 2 pkt 3 ustawy o statystyce publicznej, który ma być dodany przez art. 28 pkt 23 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych, zupełnie wyłączającego stosowanie art. 13 ust. 3 rozporządzenia unijnego (aczkolwiek w części wstępnej komentowanego art. 35h ust. 2 pkt 3 ustawy o statystyce publicznej mowa jest o ograniczeniu stosowania wymienionych niżej przepisów rozporządzenia 2016/679).

Kolejna wątpliwość Generalnego Inspektora Ochrony Danych Osobowych dotyczy art. 35h ust. 2 pkt 4 ustawy o statystyce publicznej, który ma być dodany przez art. 28 pkt 23 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych, zgodnie z którym art. 34 rozporządzenia 2016/679 stosuje się w ten sposób, że służby statystyki publicznej zamieszczają informację w Biuletynie Informacji Publicznej. Podnieść wypada, że motyw 86 rozporządzenia 2016/679 stanowi, że administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych. W świetle art. 34 ust. 1 rozporządzenia 2016/679 powyższe zawiadomienie osoby, której dane dotyczą, jest zasadą, od której wyjątkiem – przewidzianym w art. 34 ust. 3 lit. c rozporządzenia unijnego – jest możliwość zastąpienia takiego zawiadomienia publicznym komunikatem lub podobnym środkiem, gdy indywidualne zawiadomienie wymaga niewspółmiernie dużego wysiłku. W związku z tym zasadnym jest przeredagowanie zaproponowanego brzmienia art. 35h ust. 2 pkt 4 ustawy o statystyce publicznej, albowiem przepis ten, bez jakiegokolwiek uzasadnienia i wbrew art. 34 rozporządzenia 2016/679, jako jedyną formę przyjmuje zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych poprzez informację w Biuletynie Informacji Publicznej. Pamiętać należy, iż zgłaszanie naruszenia osobom, których dane dotyczą, w myśl art. 34 rozporządzenia 2016/679 następuje wyłącznie w przypadku takich naruszeń, które mogą powodować wysokie ryzyko naruszenia praw i wolności

osób, których dane dotyczą. A zatem obowiązek zawiadamiania osób, których dane dotyczą, nie dotyczy wszelkich naruszeń ochrony danych osobowych. Przepis rozporządzenia 2016/679 (art. 34) ma charakter gwarancyjny, ma stanowić realne zabezpieczenie praw osoby, której dane dotyczą, umożliwiając szybką reakcję tej osoby w przypadku zaistnienia naruszenia.

## **28. Zmiana ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2017 r. poz. 869)**

Nie może zyskać akceptacji – przewidziane w (dodawanym) art. 15c ustawy o zasadach ewidencji i identyfikacji podatników i płatników – całkowite wyłączenie stosowania art. 12–22 i art. 34 rozporządzenia 2016/679.

Trzeba po raz kolejny powtórzyć (zagadnienie to było już obszernie omawiane w uwadze do art. 95b ust. 3 ustawy o systemie oświaty oraz uwadze do art. 35h ust. 2 pkt 1 ustawy o statystyce publicznej), że w art. 23 ust. 1 rozporządzenia 2016/679 prawodawca unijny uzależnił dopuszczalność ograniczenia niektórych – przewidzianych w rozporządzeniu 2016/679 – praw i obowiązków od wykazania przez wnioskującego o takie ograniczenie, iż jest ono środkiem niezbędnym i proporcjonalnym w demokratycznym społeczeństwie, ze względu na wartości wyszczególnione w tym przepisie rozporządzenia unijnego. Wykluczył przy tym zupełne uchylenie tych praw i obowiązków w prawie państwa członkowskiego.

Takie brzmienie (projektowanego) art. 15c ustawy o zasadach ewidencji i identyfikacji podatników i płatników, jak i szczątkowy charakter uzasadnienia tej zmiany (w którym znalazły się sformułowania niemające pokrycia w zaproponowanej treści art. 15c ustawy: „Przepis zawiera ponadto [...] wymaganą przez przepisy unijne regulację zobowiązującą administratora danych do wdrożenia odpowiednich zabezpieczeń zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu danych osobowych. Przepis ten wskazuje także, że osoby, których dane dotyczą mają prawo uzyskania od administratora danych informacji, o powyższych ograniczeniach, o ile nie narusza to celu ograniczenia.”), wskazują, że projektodawca nie tylko nie ustalił, która (które) z wymienionych w art. 23 ust. 1 rozporządzenia 2016/679 wartości przemawiają za wprowadzeniem w art. 15c ustawy postulowanych wyłączeń, ale również nie przeprowadził analizy zasadności ich ustanowienia. Tym samym taki przepis nie powinien znaleźć się w projekcie ustawy –Przepisy wprowadzające ustawę o ochronie danych osobowych.

## **29. Zmiana ustawy z dnia 21 listopada 1996 r. o muzeach. (Dz. U. z 2017 r. poz. 972 i 1086)**

W opinii Generalnego Inspektora w art. 30 projektu, w którym wprowadza się zmiany do przepisu art. 2 ust. 2 ustawy o muzeach, jest zbyt ogólny. Pozwala on na przetwarzanie danych osobowych nieskonkretyzowanych kategorii osób w bardzo szerokim zakresie oraz w bardzo ogólnie określonych celach, jakimi są zadania muzeum wymienione w art. 2 ust. 1. Należałoby do poszczególnych celów przypisać kategorii osób, których dane mają być przetwarzane w adekwatnym do tego celu zakresie. Zbyt ogólna konstrukcja przepisu może prowadzić do pozyskiwania przez muzea danych osobowych w większym zakresie niż jest to niezbędne dla realizacji określonego celu. W tym samym zakresie Generalny Inspektor zgłasza uwagę do art. 6a ust. 2a.

Wyjaśnienia wymaga zasadność pozyskiwania numeru PESEL oraz rodzaju, serii i numeru dokumentu stwierdzającego tożsamość:

- a) w związku z uzgadnianiem regulaminów muzeum oraz prowadzeniem spisu uzgodnionych regulaminów (art. 6 ust. 8),
- b) w celu realizacji zadań ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego (art. 6a ust. 2a),
- c) w związku z zakupem zabytku (art. 20 ust. 5),
- d) w związku z realizacją zadań, o których mowa art. 23 ust. 1 i 2 (art. 23 ust. 2a),
- e) w związku z przenoszeniem muzealium (art. 29 ust. 1a).

W art. 6 ust. 8, art. 6a ust. 2a, art. 7 ust. 4a, art. 10 ust. 3c, art. 12a, art. 13 ust. 7, art. 19 ust. 1a, art. 19a ust. 5, art. 20 ust. 5, art. 23 ust. 2a, art. 29 ust. 1a, art. 29a ust. 3a, art. 31e ust. 3a, 33d ust. 2a, art. 33e dodawanych do ustawy, określających zakres danych osobowych przetwarzanych w poszczególnych celach, należy doprecyzować, że pozyskiwanie numeru telefonu oraz adresu poczty elektronicznej będzie miało charakter fakultatywny, np. poprzez użycie sformułowania „o ile posiada”. Posiadanie numeru telefonu oraz adresu poczty elektronicznej nie jest obligatoryjne.

Zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych budzi propozycja wyłączenia ze stosowania w ustawie o muzeach art. 5 ust. 2 rozporządzenia 2016/679 - zasady rozliczalności. Wyłączenie tej zasady jest *de facto* nie tylko wyłączeniem obowiązku stosowania i wykazywania zgodności z rozporządzeniem 2016/679 oraz wszystkich innych zasad wymienionych w art. 5 ust. 1 rozporządzenia 2016/679 o ochronie danych (zasady legalności, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności), ale też wyłączeniem wszystkich obowiązków wynikających z tego aktu prawnego. Dotyczyć to będzie np. obowiązku wdrażania odpowiednich środków technicznych i organizacyjnych związanych z odpowiednim zabezpieczeniem praw i

wolności osób, których dane dotyczą oraz wykazywaniem tego przed organem nadzorczym. Z opinii Grupy Roboczej art. 29 3/2010 w sprawie zasady rozliczalności (WP 173)<sup>8</sup> wynika, że obowiązek wdrożenia tych środków powinien mieć zastosowanie wobec administratorów danych wszystkich sektorów (publicznego i prywatnego) i powinien być skalowalny w taki sposób, aby rodzaj środków odpowiadał zagrożeniom wynikającym z przetwarzania danych i charakteru danych. Potwierdza to również art. 24 rozporządzenia 2016/679, stanowiący, że obowiązkiem administratora jest wdrożenie odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie odbywało się zgodnie z rozporządzeniem i tak aby administrator mógł to wykazać. Wprowadzając powyższe, administrator powinien uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, administrator powinien wdrożyć odpowiednie polityki ochrony danych. Niestosowanie powyższych przepisów może stanowić realne zagrożenie naruszenia praw i wolności osób, których dane dotyczą.

Generalny Inspektor zgłasza również zastrzeżenia w zakresie ograniczenia stosowania art. 12 i 15 rozporządzenia 2016/679 do ustawy o muzeach, które to projektodawca argumentuje, w uzasadnieniu, interesem finansowym państwa (minister oraz muzeum jako podmioty publiczne narażeni byłiby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń).

Artykuł 12 zakazuje administratorowi pobierania opłat za przekazanie danych osobowych, chyba że administrator wykaże, że żądania te są ewidentnie nieuzasadnione lub nadmierne „w szczególności ze względu na swój ustawiczny charakter”.

Motyw 59 rozporządzenia 2016/679 stanowi, że należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania - i gdy ma to zastosowanie bezpłatnego uzyskiwania - w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia ww. żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną. Administrator powinien być zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki - najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania - podać tego przyczyny. W zakresie wyłączeń poszczególnych przepisów rozporządzenia 2016/679, aktualna pozostaje również uwaga Generalnego Inspektora wniesiona

---

<sup>8</sup> <http://www.giudo.gov.pl/pl/1520057/3732>



do art. 2 powyższego projektu. Ponadto Grupa Robocza art. 29 w Wytycznych dotyczących prawa do przenoszenia danych (WP 242)<sup>9</sup> wskazała, że w przypadku usług społeczeństwa informacyjnego, które specjalizują się w automatycznym przetwarzaniu danych osobowych, wdrożenie zautomatyzowanych systemów takich jak interfejsy programowania aplikacji (API) może ułatwić wymianę z osobą, której dane dotyczą, i w rezultacie zmniejszyć potencjalne obciążenie wynikające z powtarzających się wniosków. Niewiele jest zatem przypadków, w których administrator danych byłby w stanie uzasadnić odmowę dostarczenia wnioskowanych informacji, nawet w odniesieniu do wielu wniosków o przeniesienie danych. Ponadto całkowity koszt procedur ustanowionych w celu udzielania odpowiedzi na wnioski o przeniesienie danych nie powinien być brany pod uwagę przy określaniu „nadmiernego charakteru” wniosku. W rzeczywistości artykuł 12 rozporządzenia 2016/679 koncentruje się na wnioskach składanych przez jedną osobę, której dane dotyczą, a nie na łącznej liczbie wniosków otrzymanych przez administratora danych. W rezultacie całkowitymi kosztami wdrożenia systemu nie można obciążać osób, których dane dotyczą, ani nie mogą one być używane do uzasadnienia odmowy udzielenia odpowiedzi na wnioski o przeniesienie.

Projektodawca powinien konstruując nowe przepisy uwzględnić argumenty wskazane w ww. wytycznych.

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi również propozycja wyłączenia stosowania w ustawie o muzeach art. 13, 14 i 15 rozporządzenia 2016/679, które w opinii organu nie znajduje uzasadnienia.

W opinii Generalnego Inspektora Ochrony Danych Osobowych doprecyzowania wymaga także kwestia ustawowego powierzania przetwarzania danych osobowych, o czy mowa w dodawanym po art. 4a ust. 7 ustawy. Przepis ustawy powinien określać, jakim podmiotom administrator danych będzie mógł powierzać przetwarzanie danych osobowych, a także w jakich konkretnych celach.

### **30. Zmiana ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2017 r. poz. 128, 777 i 966)**

Odnosząc się do art. 32 projektu, zmieniającego ustawę – Prawo o ruchu drogowym, Generalny Inspektor zauważa, że biorąc pod uwagę zasadę minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c rozporządzenia 2016/679 wskazane byłoby stworzenie zamkniętych katalogów danych,

---

<sup>9</sup> Przyjęte w dniu 13 grudnia 2016 r. i ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r., [http://www.giodo.gov.pl/1520282/id\\_art/9741/j/pl](http://www.giodo.gov.pl/1520282/id_art/9741/j/pl)

poprzez usunięcie sformułowania „w szczególności” (vide proponowane brzmienie art. 80a ust. 5 oraz art. 100a ust. 6).

Dodatkowo wskazać należy, że katalog danych przewidziany w projektowanym brzmieniu art. 80a ust. 5 różni się od zakresu uregulowanego obecnie w art. 80b ust. 1 pkt 5 ustawy – Prawo o ruchu drogowym, a zatem art. 80a ust. 5 powinien zostać sformułowany w taki sposób, aby zachowana była spójność z obowiązującymi przepisami. Podobne zastrzeżenia Generalny Inspektor zgłasza wobec zaproponowanego sformułowania art. 100a ust. 6. Wskazany w nim (otwarty) katalog danych odbiega od zakresu uregulowanego obecnie w art. 100b ust. 1 ustawy – Prawo o ruchu drogowym. Rozwiązanie takie jest w opinii organu niezrozumiałe i niedopuszczalne, bowiem przyjęcie go w zaproponowanym kształcie prowadzić będzie to wewnętrznej sprzeczności aktu prawnego.

Jednocześnie w przypadku przetwarzania danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych – mając na uwadze, że w polskim porządku prawnym nie istnieje obowiązek posiadania przez osoby fizyczne takich środków komunikacji – należy pozostawić swobodę możliwości podawania takich danych.

Wątpliwości Generalnego Inspektora wzbudzają zaproponowane przez projektodawcę szerokie wyłączenia od stosowania przepisów rozporządzenia 2016/679, polegające na zwolnieniu administratora z obowiązku informacyjnego, o którym mowa w art. 14 tego rozporządzenia odstąpieniu od stosowania art. 15 oraz art. 18 - 21 rozporządzenia 2016/679 w zakresie, w jakim dane są niezbędne do zapewnienie realizacji zadań z art. 80a i art. 100a ustawy – Prawo o ruchu drogowym. Projektodawca zdecydował się ponadto na wyłączenie stosowania art. 34 ust. 1 rozporządzenia 2016/679, jeżeli administrator danych i informacji zgromadzonych w ewidencji przetwarzający dane osobowe na potrzeby centralnej ewidencji kierowców, w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej.

Powyższe wyłączenia wymagają ponownej weryfikacji i ewentualnego dalszego doprecyzowania, w świetle argumentów przedstawionych powyżej odnośnie art. 2 oraz art. 21 projektu ustawy – Przepisy wprowadzające.

Zastrzeżenia Generalnego Inspektora budzą również kwestie terminologiczne, przepisom rozporządzenia 2016/679 nie jest bowiem znane określenie „administrator danych i informacji”.

**31. Zmiana ustawy z dnia 27 czerwca 1997 r. o bibliotekach (Dz. U. z 2012 r. poz. 642 i 908, z 2013 r. poz. 829 oraz z 2017 r. poz. 60 i 1086)**

W opinii Generalnego Inspektora w art. 33 projektu ustawy doprecyzować należy czyje dane osobowe będą przetwarzane w zakresie o którym mowa:

- a) w dodawanym do art. 6 ust. 2d w związku z powoływaniem i odwoływaniem członków Rady do Spraw Narodowego Zasobu Bibliotecznego (czy członków tej Rady, czy innych osób),
- b) w dodawanym do ustawy art. 6b,
- c) w dodawanym do art. 17 ust. 4.

W art. 6 ust. 2d art. 6b, art. 7 ust. 6a oraz w art. 17 ust. 4 – należy doprecyzować, że pozyskiwanie numeru telefonu oraz adresu poczty elektronicznej będzie miało charakter fakultatywny.

Zbyt ogólny jest także zapis art. 6b ustawy. Pozwala on na przetwarzanie danych osobowych – nieskonkretyzowanych osób – w bardzo szerokim zakresie w bardzo ogólnie określonych celach, jakimi są szeroko pojęte zadania bibliotek, wymienione w art. 4, art. 17 ust. 1 i 2, art. 18 ust.1, art. 20 ust. 1 i 2, art. 20a ust.1 i 2, art. 21 ust.1, art.22 ust. 1 i 2, art. 24, art.25 i art. 26 ustawy. Należałoby do poszczególnych celów przypisać osoby, których dane mają być przetwarzane, w adekwatnych do tego celu zakresach. Zbyt ogólna konstrukcja przepisu może prowadzić do pozyskiwania przez biblioteki danych osobowych w większym zakresie niż jest to niezbędne dla realizacji określonego celu.

Niedopuszczalnym jest również zamieszczone w art. 6b sformułowanie „w szczególności”. Pozostawienie przez ustawodawcę otwartego katalogu danych osobowych, może prowadzić do pewnej dowolności interpretacyjnej tak sformułowanych przepisów i pozyskiwania różnych, innych danych niekoniecznie bezpośrednio związanych z celem ich przetwarzania. Wyjaśnienia wymaga także zasadność pozyskiwania numeru PESEL oraz rodzaju, serii i numeru dokumentu stwierdzającego tożsamość, o którym mowa w art. 6b ustawy, w obliczu przetwarzania innych danych umożliwiających identyfikację, jak data urodzenia czy numer NIP.

W opinii Generalnego Inspektora Ochrony Danych Osobowych doprecyzowania wymaga także kwestia ustawowego powierzania przetwarzania danych osobowych, o czy mowa w dodawanym do art. 6c ust. 5 ustawy. Generalny Inspektor Ochrony Danych Osobowych w kwestii powierzania przetwarzania danych odniósł się w opinii do art. 21 niniejszego projektu.

Zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych budzi propozycja wyłączenia ze stosowania w ustawie o bibliotekach art. 5 ust. 2 rozporządzenia 2016/679 o

ochronie danych osobowych - zasady rozliczalności, a także do ograniczenia stosowania art. 12 i 15 tego rozporządzenia. Uwagi poczynione powyżej (uwagi do art. 2 oraz art. 30 projektu) na ten temat pozostają aktualne.

**32. Zmiana ustawy z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych (Dz. U. z 2016 r. poz. 358 i 2103)**

W ramach osobnej uwagi dotyczącej zmian w ustawach regulujących organizację sądów Generalny Inspektor zauważa, że regulacja przewidująca w art. 35 projektu oraz art. 52 pkt 6, art. 59 pkt 1, w związku z art. 52 pkt 6 oraz art. 58 w związku z art. 52 pkt 6 projektu ustawy ograniczenia w stosowaniu niektórych przepisów rozdziału III sekcji 1-4 rozporządzenia 2016/679 nie zawiera szczegółowych uregulowań dotyczących wszystkich niezbędnych elementów wymienionych w art. 23 ust. 2 rozporządzenia nr 2016/679 (zob. szerzej: uwagi do art. 2 oraz art. 21 projektu ustawy).

Należy również zauważyć, że przetwarzanie danych osobowych w ramach pozostałej działalności sądów nie związanej ze sprawowaniem wymiaru sprawiedliwości w myśl art. 55 ust. 3 oraz motywu 20 rozporządzenia 2016/679 podlegać będzie nadzorowi organu nadzorczego.

**33. Zmiana ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2016 r. poz. 2046 oraz z 2017 r. poz. 777, 935 i 1428)**

W art. 37 projektu, przewidującym zmiany w ustawie o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych zaproponowane brzmienie art. 6d ust. 4b wskazuje na uprawnienie do przetwarzania danych osobowych. Natomiast zgodnie z art. 6 ust. 1 lit. c rozporządzenia 2016/679 podstawą do przetwarzania może być jedynie obowiązek prawny ciążyący na administratorze. Obecna konstrukcja realizacji uprawnienia albo obowiązku wyrażona w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych nie będzie po 25 maja przyszłego roku dopuszczalna. Dlatego też konieczna jest zmiana brzmienia tego przepisu.

**34. Zmiana ustawy z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (Dz. U. z 2017 r. poz. 1277 i 1343)**

Odnosząc się do art. 38 projektu wątpliwości Generalnego Inspektora Danych Osobowych budzi projektowany art. 94b ust. 1 stanowiący, że komornik przetwarza dane osobowe stron,

uczestników postępowania oraz innych osób(...), ponieważ zawiera otwarty katalog zarówno danych osobowych przetwarzanych przez komornika, jak również podmiotów od których dane będą pozyskiwane (sformułowanie „innych osób”). Tożsama uwaga dotyczy art. 94c ust. 1 art. 94d ust. 1, w którym nie wskazano zamkniętego katalogu przetwarzanych danych.

W ocenie Generalnego Inspektora proponowane rozwiązanie jest niezgodne z zasadą minimalizacji danych określoną w art. 5 ust. 1 lit. c rozporządzenia 2016/679, którą projektodawca powinien brać pod uwagę, tworząc rozwiązania prawne związane z przetwarzaniem danych osobowych (administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych). Zasada ta powinna być respektowana przez projektodawcę odpowiedzialnego za stworzenie przepisów prawa, które będą regulować określoną materię prawną w sposób klarowny i wyczerpujący. Zatem wskazane jest dookreślenie jakie konkretnie dane (z dokładnym wskazaniem katalogu podmiotów) będą przetwarzane przez tych administratorów danych osobowych.

Generalny Inspektor zwraca uwagę, że art. 94c zawiera zarówno w ust. 1, jak i w ust. 2 sformułowania „mogą przetwarzać”, które należy zastąpić wyrazem „przetwarzają”. Sformułowanie „administrator danych osobowych” należy zastąpić pojęciem „administrator danych”.

Wątpliwości Generalnego Inspektora budzą wyłączenia stosowania przepisów rozporządzenia 2016/679 wskazane w art. 94b ust. 4 oraz art. 94 d ust. 2 i 4 (patrz: wstęp dotyczący wyłączeń). Wyłączenie zawarte w art. 94d ust. 3 stanowi powtórzenie ust. 2 tego przepisu.

Zastrzeżenia organu do spraw ochrony danych osobowych budzi art. 94 d ust. 1 stanowiący o administratorach danych (patrz uwaga ogólna dot. administratorów), który jest powtórzeniem art. 94c.

W opinii Generalnego Inspektora art. 94e wymaga doprecyzowania w zakresie okresu przechowywania danych osobowych. Zgodnie z zasadą ograniczenia przechowywania (art. 5 ust. 1 lit. e rozporządzenia 2016/679) administrator przechowuje dane nie dłużej niż jest to niezbędne do celów, w których dane te są przetwarzane.

### **35. Zmiana ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz. U. z 2016 r. poz. 187 i 1334 oraz z 2017 r. poz. 60)**

W art. 39 projektu zaproponowano dodanie art. 35 ust. 4, który stanowi, że jeżeli jest to uzasadnione zakresem usług hotelarskich, przedsiębiorcy prowadzący obiekty hotelarskie są administratorami danych osobowych klientów w tym danych osobowych dotyczących zdrowia.

Generalny Inspektor sugeruje dookreślenie sytuacji, w których – podobnie jak jest wyjaśnione w uzasadnieniu do zmian ustawy – przetwarzane będą szczególne kategorie danych osobowych – dane o stanie zdrowia. Zaprojektowany przepis art. 35 ust. 4 może stwarzać pewną dowolność interpretacyjną i podstawę prawną do pozyskiwania danych nadmiarowych w postaci m.in. danych o stanie zdrowia w sytuacji, kiedy byłoby to nieadekwatne do wykonywanych usług hotelarskich.

W odniesieniu do dodawanego art. 35a i ograniczenia zastosowania art. 14 rozporządzenia 2016/679 w ten sposób, że w celu zawarcia umowy o usługi hotelarskie, jeżeli dane niezbędne do zawarcia umowy pozyskane zostały w sposób inny niż od klientów, przedsiębiorcy prowadzący obiekty hotelarskie zobowiązani są podać klientom informacje, o których mowa w art. 14 rozporządzenia 2016/679 najpóźniej w chwili rozpoczęcia świadczenia usługi hotelarskiej. Zaproponowany przez projektodawcę przepis jest niezgodny z przepisem art. 14 ust. 3 lit. a – c rozporządzenia 2016/679, który określa terminy, w których administrator podaje informacje o których mowa w art. 14 ust. 1 i 2 osobie, której dane dotyczą. Cel powyższego ograniczenia jest niejasny, a regulacja ta nie wydaje się uzasadniona, w związku z tym, że administratorzy mają obowiązek stosować przepisy rozporządzenia 2016/679.

### **36. Zmiana ustawy z dnia 29 sierpnia 1997 – Ordynacja podatkowa (Dz. U. z 2017 r. poz. 201, 648, 768, 935 i 1428)**

W zakresie art. 40 projektu – dodawanym art. 14 § 4 – zbędnym wydaje się dookreślenie, iż minister jest administratorem danych. Użycie tego określenia powinno mieć miejsce, gdy w proces przetwarzania zaangażowana jest większa liczba podmiotów, ich rolę mogą się krzyżować albo nie będzie dochodzić do współadministrowania danymi osobowymi, o którym mowa w art. 26 rozporządzenia 2016/679.

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi także wyłączenie w art. 293 § 3 stosowania art. 12 - 22 oraz art. 34 rozporządzenia 2016/679. Zgłaszanie naruszenia osobom, których dane dotyczą, zgodnie z art. 34 rozporządzenia następuje wyłącznie w przypadku wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą. W związku z tym, obowiązek powiadamiania tych osób nie dotyczy wszelkich naruszeń. Co więcej, przepis ten ma stanowić realne zabezpieczenie i umożliwić szybką reakcję osób, których dane dotyczą w przypadku zaistnienia naruszenia. Rozporządzenie 2016/679 w art. 34 ust. 3 wskazuje sytuacje, w których zawiadomienie nie jest wymagane. W związku z powyższym w opinii Generalnego Inspektora wyłączenie stosowania art. 34 rozporządzenia 2016/679 w ustawie - Ordynacja podatkowa nie powinno mieć miejsca. W pozostałym zakresie aktualne pozostają uwagi zgłoszone

powyżej na temat ograniczania praw osób, których dane dotyczą zgodnie z art. 23 ust. 1 i 2 rozporządzenia 2016/679.

### **37. Zmiana ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2016 r. poz. 1988, z późn. zm.)**

Zastrzeżenia Generalnego Inspektora wzbudzają również regulacje zawarte w art. 41 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych.

Uwzględniając specyfikę działalności bankowej i traktowanie banków jako instytucji zaufania publicznego, jak również nie negując potencjalnej zasadności pozyskiwania przez banki informacji o karalności od niektórych pracowników banków (oraz kandydatów na pracowników na niektóre stanowiska w bankach) propozycja zamieszczona w art. 13c ust. 1 ustawy–Prawo bankowe budzi zasadnicze wątpliwości co do jej zgodności z rozporządzeniem 2016/679.

Po pierwsze – upoważnienie banków do żądania informacji o karalności od pracowników banków (kandydatów na pracowników) zostało skonstruowane zbyt szeroko pod względem podmiotowym. Użycie sformułowania, iż żądanie przedłożenia informacji o karalności jest dopuszczalne w przypadku pracownika (kandydata na pracownika): „na stanowisku umożliwiającym dostęp do danych dotyczących banku lub klientów banku” przesądza w istocie, że informacje (dane) te mogłyby być pozyskiwane od każdego pracownika (kandydata na pracownika) banku. Nie wydaje się to zgodne z zasadą minimalizacji danych –art. 5 ust. 1 lit. c rozporządzenia unijnego. Po drugie –upoważnienie banków z (projektowanego) art. 13c ust. 1 ustawy– Prawo bankowe, zostało skonstruowane zbyt szeroko pod względem przedmiotowym. Żądanie (udzielenia): „informacji czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym” oznacza umożliwienie bankowi przetwarzania informacji (danych) przekraczających kwestię karalności pracownika (kandydata na pracownika) np. danych dotyczących prawomocnego warunkowego umorzenia postępowania karnego w sprawach o przestępstwo (przestępstwo skarbowe) – art. 1 pkt 2 ustawy o Krajowym Rejestrze Karnym (Dz. U. z 2017 r. poz. 678, z późn. zm.).

W świetle powyższych rozważań zasadnym jest także pytanie, czy – skoro pozyskiwanie przez banki informacji o karalności (potencjalnie) miałoby być dopuszczalne – nie powinno być zawężone jedynie do niektórych przestępstw (np. przeciwko mieniu, obrotowi gospodarczemu i wiarygodności dokumentów, przestępstw przeciwko bezpieczeństwu powszechnemu i związanych z użyciem przemocy).

Nie wyłączać *a priori* możliwości pozyskiwania przez banki danych biometrycznych ich pracowników – zaproponowane w przepisie rozwiązania są zbyt ogólne i nie uwzględniają faktu, że dane biometryczne stanowią szczególną kategorię danych osobowych w myśl art. 9 ust. 1 rozporządzenia 2016/679.

Tak więc zanegować należy a) otwarty katalog danych biometrycznych, których banki będą mogły żądać od swoich pracowników w przypadku wejścia w życie art. 13c ust. 2 Prawa bankowego w niezmiennym kształcie, b) nieuwzględnienie wymogu z art. 9 ust. 2 pkt b rozporządzenia unijnego, zgodnie z którym przepisy prawa państwa członkowskiego dopuszczające przetwarzanie szczególnych kategorii danych osobowych (w tym danych biometrycznych) muszą przewidywać odpowiednie zabezpieczenie praw podstawowych i interesów osoby, której dane te dotyczą (w art. 13c ust. 3 Prawa bankowego poprzestano jedynie na unormowaniu okresu przechowywania danych biometrycznych, nie wskazując przy tym co stanie się z tymi danymi po dniu zakończenia zatrudnienia przez pracownika banku).

- I. Zagadnienie profilowania przez banki – art. 70 ust. 1a Prawa bankowego, który ma być dodany przez art. 41 pkt 3 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych oraz art. 105a ust. 1 Prawa bankowego w brzmieniu nadanym przez art. 41 pkt 5 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych. Istnieje zasadnicza niezgodność między dyspozycją art. 70 ust. 1a Prawa bankowego a – wydawać by się mogło dotyczącym tej samej kwestii – art. 105a ust. 1 Prawa bankowego. Pierwszy z wymienionych przepisów dopuszcza profilowanie (a nawet szerzej – przetwarzanie danych osobowych przez bank w sposób zautomatyzowany) „w celu oceny zdolności kredytowej” (oraz zapewnienia bezpieczeństwa przechowywanych środków pieniężnych – art. 50 ust. 2 w zw. z art. 70 ust. 1a Prawa bankowego). Taki cel profilowania dokonywanego przez bank jest zrozumiały, gdyż pojęcie „zdolności kredytowej” (kredytobiorcy) zostało zdefiniowane w Prawie bankowym (art. 70 ust. 1 zdanie drugie).

Tymczasem (projektowane nowe brzmienie) art. 105a ust. 1 Prawa bankowego (w pkt 1) **obok** oceny zdolności kredytowej dopuszcza profilowanie przez banki (inne instytucje ustawowo upoważnione do udzielenia kredytów oraz instytucje pożyczkowe) **również** w celu „analizy ryzyka kredytowego”. Powstaje więc pytanie odnośnie wzajemnego stosunku komentowanych przepisów oraz – co istotniejsze – **co mieści się w pojęciu analizy ryzyka kredytowego**. Wyjaśnienie tego pojęcia



wyznaczać będzie zakres dopuszczalnego profilowania prowadzonego przez banki, a zatem winno znajdować się w projektowanych przepisach Prawa bankowego.

Co więcej – o ile w oparciu o definicję z art. 70 ust. 1 zdanie drugie Prawa bankowego (oraz całe brzmienie art. 70 ust. 1 Prawa bankowego) można określić na podstawie jakich danych (informacji) profilowanie przez banki mogłoby być prowadzone, to użycie klauzuli „analiza ryzyka kredytowego” zupełnie otwiera katalog danych, które – potencjalnie – mogłyby być przez banki wykorzystywane w procesie profilowania. Powstaje zatem niebezpieczeństwo naruszenia zakazu z art. 22 ust. 4 rozporządzenia unijnego.

Niezależnie od powyższego nie może umknąć uwadze, że lakoniczność – proponowanych w projektowanych przepisach Prawa bankowego – unormowań odnoszących się do profilowania nie pozwala na jednoznaczne rozstrzygnięcie, czy banki będą prowadziły profilowanie z wykorzystaniem szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia unijnego. Przypomnieć wypada, iż kwestia przetwarzania przez banki danych szczególnie chronionych jest w istniejącym stanie prawnym przedmiotem licznych kontrowersji. Wydaje się, że przedłożona do zaopiniowania nowelizacja Prawa bankowego mogłaby stanowić okazję do rozwiania wątpliwości w tym względzie. Niestety problem ten nie znalazł odzwierciedlenia w zaprojektowanych przepisach Prawa bankowego.

**II. Art. 112b Prawa bankowego w brzmieniu nadanym przez art. 41 pkt 7 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**

Wymagają zasadniczego zakwestionowania, zawarte w art. 112b Prawa bankowego, propozycje dotyczące upoważnienia banków do przetwarzania danych biometrycznych osób fizycznych. Kwestionowany przepis jest jeszcze bardziej ogólnikowy niż (projektowany) art. 13c ust. 2 Prawa bankowego, tak pod względem wskazania osób, których dane biometryczne mogą być przetwarzane przez banki, jak i wprowadzonych zabezpieczeń praw podstawowych i interesów tych osób (patrz pkt II.). Co więcej – pomija on zupełnym milczeniem kwestię dopuszczalnego do stosowania przez banki katalogu danych biometrycznych, poprzestając na ogólnym odesłaniu do art. 4 pkt 14 rozporządzenia unijnego.

Projektowany art. 112b ust. 1 i 2 Prawa bankowego nadaje więc bankom niesłychanie szeroki zakres uprawnień do przetwarzania danych biometrycznych

(wszelkich danych biometrycznych, w ogólnie zarysowanych celach), porównywalny niemalże z uprawnieniami jakie mają w tym względzie organy ścigania wobec osób podejrzewanych o popełnienie przestępstw. Rozwiązanie to jawi się jako wysoce kontrowersyjne.

Niedopuszczalne jest przy tym, by zasadnicze kwestie dotyczące przetwarzania danych biometrycznych (a więc szczególnej kategorii danych osobowych w myśl art. 9 ust. 1 rozporządzenia unijnego) zostały przekazane do uregulowania w akcie wykonawczym – (projektowany) art. 112b ust. 3 Prawa bankowego.

- III. Nie sposób zaakceptować brzmienia (projektowanego) art. 112e ust. 1 pkt 2 Prawa bankowego. Takie całkowite wyłączenie art. 34 rozporządzenia unijnego nie jest znane przepisom tegoż rozporządzenia.

### **38. Zmiana ustawy z dnia 17 grudnia 1998 r. o zasadach użycia i pobytu Sił Zbrojnych Rzeczypospolitej Polskiej poza granicami państwa (Dz. U. z 2014 r, poz. 1510)**

W art. 42 projektu ustawy projektodawca dodaje art. 9b dokonując następujących wyłączeń stosowania przepisów rozporządzenia 2016/679, tj. obowiązków informacyjnych (art. 12 ust. 3 i 4, art. 13, art. 14), prawa usunięcia danych (art. 17), ograniczenia przetwarzania (art. 18), obowiązku poinformowania o usunięciu i ograniczeniu (art. 19), przenoszenia danych (art. 20), sprzeciwu (art. 21), automatyczne podejmowanie decyzji (art. 22), obowiązku zawiadamiania osoby o naruszeniu ochrony jej danych osobowych (art. 34).

Art. 9a dotyczy odpowiedniego stosowania przepisów art. 73 ust. 2 pkt 3, art. 74 ust. 2 pkt 7, art. 84 ust. 1a, 1aa i 1ab oraz art. 99 ust. 2 i 3 ustawy o służbie wojskowej żołnierzy zawodowych w przypadku śmierci pracownika podczas pobytu poza granicami państwa albo jeżeli pracownik zmarł w następstwie wypadku lub choroby pozostających w związku z wykonywaną pracą poza granicami państwa. W opinii Generalnego Inspektora nie wymaga regulacji, pod kątem stosowania przepisów rozporządzenia 2016/679, kwestia śmierci pracownika, o którym mowa w art. 9a. Przepisy wyłączane: art. 12 ust. 3 i 4, art. 13, art. 14, art. 17 – 22 i art. 34 rozporządzenia 2016/679 dotyczą praw osób, których dane dotyczą tzn. osób fizycznych, które mogą korzystać z praw przewidzianych w Rozdziale III rozporządzenia 2016/679, a nie osób zmarłych.

### **39. Zmiana ustawy z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka (Dz. U. z 2017 r. poz. 922)**

Generalny Inspektor zwraca uwagę, że przewidziane w art. 45 projektowanej ustawy brzmienie art. 10c ustawy o Rzeczniku Praw Dziecka budzi wątpliwości z uwagi na zastosowanie wyrażenia „może przetwarzać wszelkie informacje” (ust. 1) oraz „może przetwarzać dane osobowe”, co do zgodności z art. 51 ust. 2 Konstytucji oraz art. 5 ust. 1 lit. c rozporządzenia 2016/679 (szerzej: uwagi do art. 15 projektu ustawy).

#### **40. Zmiana ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2017 r. poz. 678)**

Jak było to już kilkakrotnie podnoszone (m.in. w uwadze do art. 95b ust. 3 ustawy o systemie oświaty oraz uwadze do art. 35h ust. 2 pkt 1 ustawy o statystyce publicznej) prawodawca unijny w art. 23 ust. 1 rozporządzenia 2016/679 uzależnił dopuszczalność ograniczenia niektórych – przewidzianych w rozporządzeniu – praw i obowiązków od wykazania przez wnioskującego o takie ograniczenie, iż jest ono środkiem niezbędnym i proporcjonalnym w demokratycznym społeczeństwie, służącym: a) bezpieczeństwu narodowemu, b) obronie, c) bezpieczeństwu publicznemu, d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom, e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu, f) ochronie niezależności sądów i postępowania sądowego, g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu, h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)–e) oraz g), i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób, j) egzekucji roszczeń cywilnoprawnych.

W projektowanych – art. 46 pkt 1 lit. a i 2 projektu ustawy – Przepisy wprowadzające– art. 4 ust. 3 i art. 8 ust. 3a ustawy o Krajowym Rejestrze Karnym projektodawca ograniczył się do lakonicznego stwierdzenia, iż określonych przepisów rozporządzenia 2016/679 nie stosuje się. Brak jest zatem wskazania, która (które) z wymienionych w art. 23 ust. 1 rozporządzenia 2016/679 wartości przemawiają – w opinii projektodawcy – za

wprowadzeniem przedmiotowych wyłączeń w ustawie o Krajowym Rejestrze Karnym. Wątpliwe jest, czy projektodawca przeprowadził analizę zasadności ustanowienia tych wyłączeń, skoro w powoływanych wyżej przepisach ustawy o Krajowym Rejestrze Karnym zaproponował wyłączenie art. 21 rozporządzenia 2016/679, który to przepis w ogóle nie znajduje zastosowania do przetwarzania danych osobowych na potrzeby Krajowego Rejestru Karnego.

**41. Zmiana ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. z 2013 r. poz. 1222, z 2015 r. poz. 201 oraz z 2017 r. poz. 1442)**

W odniesieniu do dodanego w art. 1 ust. 8 do ustawy o spółdzielniach mieszkaniowych, wskazać trzeba, że w ocenie Generalnego Inspektora umieszczenie tego przepisu jest zbędne ze względu na to, iż to spółdzielnia przetwarza dane osobowe jej członków oraz osób niebędących jej członkami zgodnie z celami i na zasadach określonych w cytowanej ustawie.

**42. Zmiana ustawy z dnia 3 lutego 2001 r. o ochronie dziedzictwa Fryderyka Chopina (Dz. U. poz. 168)**

W odniesieniu do art. 48 projektu, który wprowadza zmiany w ustawie o ochronie dziedzictwa Fryderyka Chopina, wątpliwości Generalnego Inspektora budzi przetwarzanie danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych (art. 5a ust. 1 oraz art. 6 ust. 4 pkt 1 ustawy) oraz imion rodziców danej osoby, daty i miejsca jej urodzenia (ust. 2 każdego z wyżej wskazanych artykułów). Argumentacja w tym zakresie została wskazana przy okazji uwag do art. 21 projektu. Natomiast, jeżeli intencją projektodawcy było to żeby numer telefonu i adres poczty elektronicznej miały charakter danych związanych z wykonywaniem pracy, zadań służbowych to należy dookreślić ich charakter poprzez dodanie wyrażenia „służbowy/a”.

Kolejną uwagę Generalny Inspektor kieruje do okresów przechowywania danych wymienionych w 5a ust. 1 oraz art. 6 ust. 4 pkt 1 ustawy o ochronie dziedzictwa, które w obu przypadkach wynoszą 80 lat. Zgodnie z motywem 39 rozporządzenia 2016/679 aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien zapewnić ograniczenia okresu przechowywania danych do ścisłego minimum, czyli ustalić termin ich usuwania lub okresowego przeglądu. W związku z powyższym Generalny Inspektor podaje pod ponowną rozagę projektodawcy, czy taki okres przechowywania danych będzie adekwatny do realizacji celów administratorów. Jeżeli projektodawca uzna jednak, że jest to konieczne - Generalny Inspektor sugeruje ustalenie obowiązku dokonywania okresowego przeglądu w celu oceny przydatności takich danych.

Kolejną uwagę Generalny Inspektor zgłasza do art. 6 ust. 3 ustawy o ochronie dziedzictwa, który stanowi, że Instytut może zlecać przetwarzanie w jego imieniu danych osobowych lub pełnić funkcję podmiotu przetwarzającego dane osobowe na zlecenie innego podmiotu. Takie brzmienie przepisu należy uznać za niezgodne z rozporządzeniem 2016/679. Właściwa w tym przypadku będzie argumentacja zamieszczona w art. 21 projektu.

W odniesieniu do art. 6 ust. 7 i 8 ustawy o ochronie dziedzictwa Generalny Inspektor zauważa, że w celu opiniowania wniosków o nadanie odznaki i rekomendowania ministrowi osób lub jednostek organizacyjnych do nadania odznaki tworzy się komisję. Komisja ta będzie zatem przetwarzać dane osobowe we wnioskach, dlatego słuszne wydaje się wskazanie wprost w przepisach, że obsługę administracyjno - biurową komisji zapewnia minister właściwy do spraw kultury i dziedzictwa narodowego.

Zgodnie z projektowanym art. 6 ust. 10 zmienianej ustawy informacje o odznakach podaje się do publicznej wiadomości w Biuletynie Informacji Publicznej na stronie podmiotowej ministra. Zatem, Generalny Inspektor sugeruje określenie adekwatnego katalogu danych osób, którym nadane zostały odznaki, które mają zostać upublicznione.

Projektowany art. 6a ust. 1 ustawy powiela postanowienia treści art. 23 ust. 2 lit. d rozporządzenia 2016/679 zatem aktualna pozostaje argumentacja przedstawiona do art. 21 projektu.

W odniesieniu do zastosowanych w art. 6a ust. 2 - 4 ograniczeń należy zauważyć, że nie wydaje się słuszne ograniczanie praw, o których mowa w art. 12, 14, 15 i 19 rozporządzenia 2016/679 ze względu na interes finansowy państwa, co wskazane zostało również w argumentacji do art. 21 projektu.

Kolejna wątpliwość Generalnego Inspektora dotyczy treści art. 6a ust. 5, zgodnie z którym nie stosuje się art. 34 rozporządzenia 2016/679 jeżeli administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej. Argumentację przeciwko zastosowaniu takiej konstrukcji prawnej Generalny Inspektor przedstawił szczegółowo do art. 21 projektu.

**43. Zmiana ustawy z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego (Dz. U. z 2016 r. poz. 1610 oraz z 2017 r. poz. 1442)**

Odnosnie art. 50 projektu, w ocenie Generalnego Inspektora Ochrony Danych Osobowych wątpliwości budzą rozwiązania dotyczące przyznawania lokali z mieszkaniowego zasobu gminy lub innej jednostki samorządu terytorialnego.

Kierunkowo wskazać należy, iż wymienione w ustawie o ochronie praw lokatorów „uchwały organu stanowiącego jednostki samorządu terytorialnego, zarządzenia wojewody lub uchwały organu wykonawczego państwowej osoby prawnej” - które zgodnie z ustanowionym w Konstytucji RP systemem źródeł prawa mają powszechnie obowiązujący charakter na ograniczonym obszarze - nie mogą jednak stanowić podstawy do przetwarzania danych osobowych, w szczególności przetwarzania danych wrażliwych, w miejsce nieistniejących lub niedoskonałych przepisów prawa. Uchwały przewidują również, przy przyznawaniu lokali z mieszkaniowego zasobu gminy lub innej jednostki samorządu terytorialnego przeprowadzanie wywiadu środowiskowego w miejscu zamieszkania w okresie 5 lat przed złożeniem wniosku. Wspomniany wywiad środowiskowy obejmuje zbadanie sytuacji materialnej osób pozostających we wspólnym pożyciu, ich sytuacji życiowej i rodzinnej, a co za tym idzie, przetwarzania danych tzw. zwykłych oraz danych wrażliwych /szczególnych kategorii danych/ tych osób. Ważny w tym kontekście wydaje się również okres weryfikacji tych danych, ich przetwarzania oraz przechowywania, który powinien być wyraźnie wskazany.

Rozwiązania zawarte w ustawie są w ocenie Generalnego Inspektora niezgodne zasadami dotyczącymi przetwarzania danych osobowych przewidzianych w art. 5 ust. 1 lit. a, b oraz c rozporządzenia 2016/679. Dlatego też Generalny Inspektor sugeruje przyjęcie – z uwzględnieniem zasad wynikających z rozporządzenia 2016/679 - w powszechnie obowiązujących przepisach prawa norm stanowiących podstawę prawną dokonywania przedmiotowej oceny oraz wyznaczenie tymi przepisami zasad i kryteriów jej dokonywania w procesie przyznawania lokali z mieszkaniowego zasobu gminy lub innej jednostki samorządu terytorialnego.

#### **44. Zmiana ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2016 r. poz. 2062, z późn. zm.)**

Generalny Inspektor zwraca uwagę, że w przewidzianych w art. 52 pkt 1, 2 i 3 projektu ustawy wyłączeniach stosowania art. 13-15 ust. 1 i 3, art. 18, art. 19 i art. 21 oraz art. 16 rozporządzenia nr 2016/679 w art. 157 § 2b i § 2d, art. 157ea § 2 i 4, art. 168a § 2 i 4 ustawy nie przewidziano przepisów szczególnych czyniących zadość wszystkim wymaganiom określonym w art. 23 ust. 2 rozporządzenia 2016/679 (szerzej: uwagi do art. 2 oraz art. 21 projektu ustawy).

W ramach osobnej uwagi dotyczącej zmian w ustawach regulujących organizację sądów Generalny Inspektor zauważa, że regulacja przewidująca w art. 52 pkt 6, art. 59 pkt 1, art. 35 w związku z art. 52 pkt 6 oraz art. 58 w związku z art. 52 pkt 6 projektu ustawy ograniczenia w stosowaniu niektórych przepisów rozdziału III sekcji 1-4 rozporządzenia 2016/679 nie zawiera szczegółowych regulujących wszystkie niezbędne elementy wymienione w art. 23 ust. 2 rozporządzenia 2016/679 (szerzej: uwagi do art. 2 oraz art. 21 projektu ustawy).

Należy również zauważyć, że przetwarzanie danych osobowych w ramach pozostałej działalności sądów nie związanej ze sprawowaniem wymiaru sprawiedliwości w myśl art. 55 ust. 3 oraz motywu 20 rozporządzenia 2016/679 podlegać będzie nadzorowi organu nadzorczego.

#### **45. Zmiana ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U z 2016 r. poz. 1483i 1948)**

Organ do spraw ochrony danych osobowych zgłasza uwagę do projektowanych przepisów art. 8a ustawy o Żandarmerii i wojskowych organach porządkowych dotyczących przetwarzania danych osobowych w zakresie przeprowadzonych postępowań kwalifikacyjnych osób ubiegających się o przyjęcie do służby lub pracy w Żandarmerii Wojskowej. Przepis ten nie zawiera postanowień dotyczących retencji danych (okresu przechowywania i ich usuwania) w stosunku do osób, które nie przeszły pozytywnie postępowania kwalifikacyjnego. W związku z powyższym Generalny Inspektor wnioskuje o uregulowanie tej kwestii w przepisach ustawy.

Generalny Inspektor pragnie zauważyć, że ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych określa zakres działania i organizację Żandarmerii Wojskowej oraz rodzaje i zadania wojskowych organów porządkowych (w tym uprawnienia i obowiązki odpowiednio żołnierzy Żandarmerii Wojskowej oraz żołnierzy organów porządkowych). Przepisy te, na wzór ustawy o Policji formułują m.in. uprawnienia żołnierzy Żandarmerii Wojskowej związane z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych oraz ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom odpowiadają niejako uprawnieniom Policji w odniesieniu do m.in. żołnierzy pełniących czynną służbę wojskową i niebędących w czynnej służbie oraz innych osób wymienionych w art. 3 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Zgodnie z powyższym organ do spraw ochrony danych osobowych sugeruje analizę przedmiotowej ustawy pod kątem 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 uchyłającą decyzję ramową Rady 2008/977/WSiSW, której przepisy dotyczące transpozycji zobowiązują państwa członkowskie do przyjęcia i publikacji do dnia 6 maja 2018 r. przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do jej wykonania.

#### **46. Zmiana ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2016 r. poz. 1907, 1935 i 1948 oraz z 2017 r. poz. 708 i 1214)**

W art. 55 projektu należy zgłosić analogiczną uwagę jak powyższa do art. 25 projektu, w zakresie propozycji ujętych w art. 51 ust. 9 oraz art. 55a ust. 1.

Dodatkowo zastosowanie mają uwagi o nowych uprawnieniach Inspekcji Transportu Drogowego (art. 55a) poczynione uprzednio w toku konsultacji z Ministerstwem Finansów<sup>10</sup>.

W zakresie nowego brzmienia art. 82 ustawy o transporcie drogowym aktualne pozostaje stanowisko co do realizacji obowiązku informacyjnego, o którym mowa powyżej<sup>11</sup>.

#### **47. Zmiana ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2016 r. poz. 1030 i 1579)**

W art. 57 pkt 5 - 9 projektu zaproponowano uchylenie przepisów implementujących postanowienia dyrektywy 2002/58<sup>12</sup> w związku z brzmieniem motywu 173 oraz art. 95 rozporządzenia 2016/679. Jednocześnie w przepisach tych nie wskazano, by konieczne było zmienianie prawa krajowego, a jedynie, iż dyrektywa 2002/58 powinna zostać dostosowana po przyjęciu rozporządzenia. Proces ten już się rozpoczął – trwają prace nad projektem tzw. rozporządzenia e-privacy<sup>13</sup>. W takiej sytuacji projektodawca powinien rozważyć, czy konieczna jest zmiana i uchylenie przepisów ujętych w pkt 5-9 art. 57.

---

<sup>10</sup> Sygn. DOLiS-023-407/17/KK/68668,68675,68676 z 13 września 2017 r., <http://www.giodo.gov.pl/pl/1520275/10186>

<sup>11</sup> Sygn. DOLiS-023-237/17/KK/46501 z 7 czerwca 2017 r., DOLiS-023-237/17/KK/56240 z 17 lipca 2017 r., <http://giodo.gov.pl/pl/1520275/10119>

<sup>12</sup> Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

<sup>13</sup> Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchyłające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final 2017/0003(COD)



**48. Zmiana ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz. U. z 2016 r. poz. 2060 oraz z 2017 r. poz.1089)**

W art. 60 projektu ustawy– nie wskazano jakie dane albo kategorie danych mają być przetwarzane w zakresie niezbędnym do wykonywania wskazanych w tej jednostce redakcyjnej przepisów. Część z powołanych tam przepisów zawiera katalogi danych. W związku z powyższym, celem uniknięcia dopuszczenia przetwarzania nieograniczonego zakresu danych, należy wskazać takie dane albo ich kategorie w powiązaniu z zadaniami wykonywanymi przez Fundusz. Projektodawca powinien także zweryfikować, czy wszystkie kategorie danych wskazane w katalogach nowo projektowanego ust. 7 komentowanego przepisu są niezbędne do wykonywania wskazanych w przepisie zadań. Analogiczne uwagi należy zgłosić do proponowanego art. 136a.

Projektowany art. 98a może być niezgodny z treścią art. 23 rozporządzenia 2016/679, w zakresie w jakim w sposób całkowity ogranicza prawa osób, których dane dotyczą do bezpłatnego wykonywania przysługujących im praw raz na sześć miesięcy a jednocześnie nie reguluje kwestii ujętych w art. 23 ust. 2 rozporządzenia 2016/679. Projektodawca nie wskazał, czy dotychczas funkcjonujący 6-miesięczny okres jest zgodny z normami rozporządzenia 2016/679. Trudno sobie wyobrazić np. by podmiot danych mógł żądać poprawienia albo usunięcia danych tylko raz na pół roku, a za kolejne próby miał ponosić koszty. Dodatkowo należy zauważyć, iż opłata w ma być „rozsądnej wysokości”, ale już bez określenia „wynikającej z kosztów administracyjnych”, jak stanowi art. 15 ust. 3 rozporządzenia 2016/679. W związku z tym ocena, co praktycznie oznacza opłata w „rozsądnej wysokości”, będzie nastroczała wielu trudności. Analogiczne uwagi należy zgłosić do proponowanego art. 136b.

W projektowanym art. 98b zaproponowano całkowite wyłączenie obowiązku informowania o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, wykorzystaniu danych osobowych do innego celu, niż ten w którym zostały zebrane, powiadomieniu o sprostowaniu lub usunięciu danych lub ograniczeniu przetwarzania oraz zgłaszaniu naruszeń ochrony danych, jeżeli spowodowałoby to nadmierny koszt po stronie Funduszu. Tak szerokie wyłączenie ograniczać będzie, nie tylko prawa osoby, której dane dotyczą, ale także uprawnienia nadzorcze organu ochrony danych. Żadne z tak daleko idących rozwiązań nie może zostać zaakceptowane. Niezrozumiałym jest przyzwolecie na taką sytuację z powodu nadmiernych kosztów po stronie Funduszu. Organ nadzorczy powinien być informowany o stwierdzonych naruszeniach ochrony danych niezależnie od związanych z tym kosztów. Uzasadnienie projektu milczy na ten temat. Analogiczne uwagi należy zgłosić do proponowanego art. 136c.

Nowy art. 98c dopuszczający profilowanie nie przewiduje środków ochrony praw, wolności i prawnie uzasadnionych interesów osób, których dane dotyczą. W tym zakresie przepis może być niezgodny z art. 22 ust. 2 lit. b rozporządzenia 2016/679. Należy pamiętać, iż podstawowym prawem podmiotu danych jest niepodleganie decyzji opartej na zautomatyzowanym przetwarzaniu. W braku takiej możliwości jego prawa muszą być zagwarantowane w przepisach szczególnych. Analogiczne uwagi należy zgłosić do proponowanego art. 136d.

O ile wątpliwości w proponowanym art. 98d nie budzi dopuszczenie możliwości zlecenia przetwarzania innym podmiotom, to niejasnym jest w jakim zakresie miałby Fundusz być podmiotem przetwarzającym dane na zlecenie innego podmiotu. Kwestia ta wymaga dalszego wyjaśnienia i doprecyzowania.

#### **49. Zmiana ustawy z dnia 13 czerwca 2003 r. o zatrudnieniu socjalnym (Dz. U. z 2016 r. poz. 1828)**

W art. 61 projektu odnoszącym się do zmian ustawy o zatrudnieniu socjalnym, należy – biorąc pod uwagę zasadę minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c rozporządzenia 2016/679 – stworzyć zamknięty katalog przetwarzanych danych, poprzez usunięcie sformułowania „w szczególności” (*vide* proponowane brzmienie art. 8 ust. 1).

Wątpliwości Generalnego Inspektora budzą zaproponowane przez projektodawcę szerokie wyłączenie od stosowania przepisów rozporządzenia 2016/679, polegające na ogólnie sformułowanym zwolnieniu administratora z obowiązku stosowania art. 13-15 ust. 1 i 3, art. 18, art. 19 oraz art. 21 rozporządzenia 2016/679. Zagadnienie to wymaga ponownej weryfikacji i ewentualnego dalszego doprecyzowania, w świetle argumentów przedstawionych powyżej odnośnie do art. 2 oraz art. 21 przepisów wprowadzających.

Odnosząc się do projektowanych art. 8b ust. 6 oraz 18d ust. 6 ustawy o zatrudnieniu socjalnym, Generalny Inspektor zauważa, iż okres retencji danych sformułowany został w sposób nieprecyzyjny, umożliwia bowiem swobodne kształtowanie okresu przechowywania danych przez podmiot publiczny, który powinien działać na podstawie przepisów prawa, sugeruje się zatem jego dookreślenie.

#### **50. Zmiana ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami (Dz. U. z 2014 r. poz. 1446, z późn. zm.)**

Projektowany art. 6a ust. 1 ustawy powiela postanowienia treści art. 23 ust. 2 lit. d rozporządzenia 2016/679. Zatem aktualna pozostaje argumentacja przeciw takiemu rozwiązaniu z art. 21 projektu.

W odniesieniu do zastosowanych w art. 6a ust. 2-5 ograniczeń należy zauważyć, że nie wydaje się słuszne ograniczanie praw, o których mowa w art. 12, 13, 14, 15, 16, 18-20 rozporządzenia 2016/679 ze względu na interes finansowy państwa, co Generalny Inspektor w wskazuje również w art. 21 projektu.

Na podstawie art. 6a ust. 6 nie stosuje się art. 34 rozporządzenia 2016/679 jeżeli administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej. W kwestii nieprawidłowości konstrukcji tego przepisu Generalny Inspektor odniósł się w uwagach do art. 21 projektu.

Koncepcja „zlecania przetwarzania”, o której mowa w art. 6a ust. 7 została podważona w argumentacji do art. 21 projektu.

Przepisem art. 62 pkt 2 – 31 projektu projektodawca dookreślił administratorów oraz zakres przetwarzanych przez nich danych. W związku z powyższym wątpliwości Generalnego Inspektora budzi przetwarzanie danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych (art. 5a ust. 1 oraz art. 6 ust. 4 pkt 1 ustawy o ochronie dziedzictwa) a zatem aktualna również i w tym przypadku pozostaje argumentacja do art. 21 projektu.

#### **51. Zmiana ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz. U. z 2016 r. poz. 1726 i 2138 oraz z 2017 r. poz. 60)**

W art. 63 projektu projektodawca zakłada utworzenie katalogu otwartego danych osobowych o stanie zdrowia poprzez użycie sformułowania „w szczególności”. W opinii Generalnego Inspektora Ochrony Danych Osobowych zakres danych osobowych określony w ustawie powinien stanowić katalog zamknięty. Przepis ten wymaga przeredagowania w tym zakresie.

#### **52. Zmiana ustawy z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego (Dz. U. z 2017 r. poz. 1453)**

W ocenie Generalnego Inspektora Ochrony Danych Osobowych zakres danych wymieniony w art. 64 projektu – w dodawanym art. 43 ust. 1a ww. ustawy – jest zbyt szeroki i nieadekwatny do celu przetwarzania danych. Wskazać należy, iż proponowany zapis art. 43 ust. 1a pkt 3 – adres

miejsca zamieszkania lub adres do korespondencji wymaga doprecyzowania. Zasadne wydaje się zastąpienie wyrazu „lub” wyrazem „albo”, gdyż sugeruje on podanie nie tylko adresu zamieszkania ale również adresu do korespondencji i nie jest określeniem wyraźnym wskazującym na podanie jednej bądź drugiej z wymienionych danych. Adres zamieszkania jako dana osobowa przetwarzana przez administratora, przy jednoczesnym fakultatywnym (warunkowym) wskazaniu adresu do korespondencji rodzi pytanie o niezbedność przetwarzania tych danych, a tym samym zgodność z zasadą minimalizacji danych wynikającą z art. 5 ust. 1 lit. c rozporządzenia 2016/679. Podobnie podanie numeru telefonu oraz adresu e-mail (pkt 3 ww. przepisu) na zasadzie obowiązku nie znajduje uzasadnienia, bowiem obowiązek posiadania numeru telefonu, czy adresu poczty elektronicznej nie wynika wprost z obowiązujących przepisów polskiego prawa. Podanie numeru telefonu można wskazać jako rozwiązanie fakultatywne, a nie obligatoryjne. Niezbedność udostępnienia i dalszego przetwarzania tych danych nie została przez projektodawcę wykazana, dlatego też taki zakres należy uznać za nadmierny.

Proponowane rozwiązanie zawarte art. 43 ust. 1a jest w ocenie Generalnego Inspektora niezgodne z zasadą minimalizacji danych, którą projektodawca powinien brać pod uwagę tworząc rozwiązania prawne związane z przetwarzaniem danych osobowych. Zgodnie z treścią powyższego przepisu administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były adekwatne, stosowne oraz ograniczone do tego, co jest niezbedne w stosunku do celów, w jakich są przetwarzane.

W zakresie propozycji ujętej w ust. 1b aktualne pozostają uwagi zgłoszone do art. 21 projektu dotyczące instytucji powierzenia danych osobowych.

Wątpliwości Generalnego Inspektora budzi również przepis art. 43 ust. 1c wymagający doprecyzowania ze względu na zasadę ograniczenia przechowywania (art. 5 ust. 1 lit. e rozporządzenia 2016/679)– „okres niezbedny do realizacji zadań, obowiązków i uprawnień” oraz zasadę integralności i poufności (art. 5 ust. 1 lit. c rozporządzenia 2016/679) – „dane, o których mowa w ust. 1a podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi”. Należy wskazać, iż ustawodawca powinien uściślić (dookreślić) przepisy związane z wyżej wspomnianymi zasadami w ramach projektu ze względu na okres ich przechowywania, nie dłuższy niż jest to niezbedne do celów, w których dane te są przetwarzane oraz ze względu na niezbedność przetwarzania tych danych.

Kolejna wątpliwość Generalnego Inspektora dotyczy treści art.43 ust. 1f oraz 1g, zgodnie z którymi nie stosuje się art. 34 rozporządzenia 2016/679, jeżeli administrator w terminie 72

godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynu Informacji Publicznej lub na swojej stronie internetowej.

**53. Zmiana ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2016 r. poz. 1518, z późn. zm.)**

W art. 65 projektu ustawy, w zakresie zmiany brzmienia art. 23 ust. 9 ww. ustawy, organ do spraw ochrony danych wskazuje, iż przepis ten zawiera odniesienie do przepisów o ochronie danych osobowych. Generalny Inspektor przypomina, iż przepisy o ochronie danych osobowych jako przepisy ogólne mają zastosowanie, niezależnie od odesłań znajdujących się w omawianych przepisach ustaw. Takie odesłania nie określają także w sposób wystarczający zasad przetwarzania danych przez ministra oraz upoważnione podmioty. To w tych przepisach szczególnych powinny być określone wyczerpująco zasady przetwarzania danych przez administratora oraz podmioty, którym udostępniane są dane, w szczególności tryb pozyskiwania, udostępniania i przechowywania danych. Ogólne odesłanie do przepisów o ochronie danych osobowych może rodzić wątpliwości co do zasad przetwarzania danych mających zastosowanie.

Wątpliwości budzi także projektowany art. 23 ust. 11 i 12 ustawy, tj. określony w tych przepisach ustawy okres przechowywania informacji przez ministra do spraw rodziny w rejestrze centralnym, oraz przez podmioty, wymienione w ust. 10, którym dane z rejestru centralnego zostały udostępnione. Okres ten wynosi 10 lat od dnia zaprzestania udzielania świadczeń albo 10 lat od dnia ich udostępnienia z rejestru centralnego uprawnionym organom oraz 1 roku w przypadku, gdy świadczenie nie zostało przyznane. W ocenie organu do spraw ochrony danych osobowych jest to sprzeczne z podstawową zasadą ograniczenia przechowywania wynikająca z art. 5 ust. 1 pkt e rozporządzenia 2016/679.

**54. Zmiana ustawy z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2016 r. poz. 930, z późn. zm.)**

W art. 66 projektu wątpliwości budzi dodany w art. 100 ust. 3 – 7 ustawy o pomocy społecznej, który reguluje wyłączenie przepisów art. 13 – 15 ust. 1 i 3, 18, 19 i 21 rozporządzenia 2016/679, w stosunku do osób ubiegających się i korzystających ze świadczeń pomocy społecznej. W odniesieniu do tej propozycji Generalny Inspektor wnosi ogólną uwagę w zakresie zgłoszonym na początku pisma co do niedopuszczalnego i niezasadnego stosowania wyłączeń stosowania przepisów rozporządzenia 2016/679 w zakresie praw podmiotów danych.

Ponadto, zauważyć należy niespójność pomiędzy prawem do korzystania przez osoby wnioskujące o przyznanie konkretnego świadczenia z zakresu pomocy społecznej, czyli strony postępowania do uprawnień kontrolnych wynikających z rozporządzenia 2016/679, a uprawnieniem strony do realizowania wglądu do akt postępowania administracyjnego, wynikające z 73 i 74 Kodeksu postępowania administracyjnego. Takie opracowanie przepisów ww. ustawy powoduje brak wzajemnej korelacji przepisów ustawy o pomocy społecznej i Kodeksu postępowania administracyjnego w zakresie praw i uprawnień przysługującej stronie postępowania administracyjnego o przyznanie świadczenia z zakresu pomocy społecznej.

W odniesieniu do dodawanego art. 100 ust. 6 zwrócić uwagę należy na konieczność dookreślenia i doprecyzowania w tym przepisie jakie „procedury prawne dotyczące zabezpieczeń zapobiegającym nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu” projektodawca miał na myśli, tj. wyraźnego wskazania wymaga jakie inne procedury prawne niż wynikające z rozporządzenia 2016/679 miałyby to być. Zwrócić uwagę należy, że procedury zabezpieczeń zapobiegających nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu nie mogą być wprowadzane w zakresie innym, a tym bardziej mniejszym niż wynikający z przepisów rozporządzenia.

W odniesieniu do dodanego art. 100 ust. 7 zmienianej ustawy należy zwrócić uwagę na brak wskazania okresu przechowywania danych osobowych. Jest zbyt lakonicznym wskazanie, iż okres przechowywania ustala administrator zgodnie z celami ich przetwarzania. W ocenie organu do spraw ochrony danych osobowych takie brzmienie przepisu jest to sprzeczne z podstawową zasadą rozporządzenia 2016/679, tj. zasadą ograniczenia przechowywania wynikająca z art. 5 ust. 1 pkt e rozporządzenia.

#### **55. Zmiana ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2016 r. poz. 1829, z późn. zm.)**

W art. 68 pkt 1 projektu zbędnym wydaje się dookreślenie, iż minister jest administratorem. Użycie tego określenia powinno mieć miejsce, gdy w proces przetwarzania zaangażowana jest większa liczba podmiotów, ich rolę mogą się krzyżować albo nie będzie dochodzić do współadministrowania danymi osobowymi, o którym mowa w art. 26 rozporządzenia 2016/679.

Zgodnie z treścią uzasadnienia propozycje ujęte w tym artykule były przedmiotem uzgodnień pomiędzy Ministrem Rozwoju a organem do spraw ochrony danych osobowych w ramach prac nad tzw. Konstytucją dla Biznesu, w szczególności nad projektem ustawy o Centralnej

Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy<sup>14</sup>. Generalny Inspektor prosi o zweryfikowanie, czy tożsame do proponowanych zmian postanowienia nie będą wcześniej uchwalone w tych bardziej zaawansowanych procesach legislacyjnych. Jest to w szczególności uzasadnione z uwagi na fakt, iż przepisy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej zostały w ramach prac wyłączone z ustawy o swobodzie działalności gospodarczej do odrębnego projektu ustawy.

**56. Zmiana ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, z późn. zm.)**

W zakresie art. 69 pkt 1 lit. b projektu należy zauważyć, że proponowana regulacja może końcowych do niepodlegania takim rozstrzygnięciom zgodnie z art. 22 ust. 1 rozporządzenia 2016/679. Po drugie, powtórzenie treści przepisu art. 22 ust. 2 lit. b rozporządzenia 2016/679 nie spełnia wymogu stworzenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. To po stronie ustawodawcy, a nie dostawcy usług, leży obowiązek stworzenia prawnych gwarancji dla użytkownika końcowego. Powinny one zostać określone w akcie prawa powszechnego, a nie na przykład wewnętrznych regulacji dostawcy usług. W razie uznania i uzasadnienia niezbędności stosowania tego typu profilowania, w przepisach Prawa telekomunikacyjnego należy przewidzieć mechanizmy zabezpieczające prawa odbiorcy końcowego.

Zmiany wprowadzane w pkt 4 komentowanego artykułu prowadzą do zmiany zakresu przetwarzanych danych osobowych – zawierają dopuszczenie przetwarzania innych danych na podstawie przepisów o ochronie danych osobowych. Odniesienie takie nie reguluje, inaczej niż w obecnej sytuacji, dopuszczalnego przepisami prawa zakresu przetwarzanych danych. Nie ustalono żadnych szczegółowych zasad. Uzasadnienie nie zawiera wyjaśnienia w tym zakresie.

**57. Zmiana ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. z 2016 r. poz. 1793, z późn. zm.)**

Odnosząc się do art. 70 projektu, dotyczącego zmian w ustawie o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, Generalny Inspektor, w pierwszej kolejności zwraca uwagę na projektowany art. 188 ust. 2d, który stanowi, iż do przetwarzania danych osobowych przez Narodowy Fundusz Zdrowia przepisu art. 14 ust. 1-4 rozporządzenia 2016/679 nie stosuje się. Zauważyć należy, że zgodnie z art. 14 ust. 5 lit. c rozporządzenia 2016/679, ust. 1–4

---

<sup>14</sup> <http://legislacja.rcl.gov.pl/projekt/12295218/katalog/12416282#12416282>

nie mają zastosowania, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą. Generalny Inspektor sugeruje zatem doprecyzowanie art. 188 ust. 2d, w taki sposób, aby odpowiadał on wymogom wskazanym w art. 14 ust. 5 lit. c rozporządzenia 2016/679.

W zaproponowanym brzmieniu art. 188b oraz art. 191 ust. 2 użyto sformułowań wskazujących na uprawnienie Funduszu oraz ministra właściwego do spraw zdrowia do przetwarzania danych osobowych. Natomiast zgodnie z art. 6 ust. 1 lit. c rozporządzenia 2016/679 podstawą do przetwarzania może być jedynie obowiązek prawny ciążyący na administratorze. Obecna konstrukcja realizacji uprawnienia albo obowiązku wyrażona w art. 23 ust. 1 lit. b ustawy o ochronie danych osobowych nie będzie po 25 maja przyszłego roku dopuszczalna. Dlatego też konieczna jest zmiana brzmienia przepisów.

#### **58. Zmiana ustawy z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego (Dz. U. z 2016 r. poz. 1222 i 1579)**

Wątpliwości budzi konkretne wskazywanie w projektowanym art. 29a ust. 1 podmiotów, które pełnią rolę administratora. Jak widać z przedłożonego projektu jest to podyktowane zakresem ustawowo uregulowanych kompetencji i wykonywanych zadań przez te podmioty, jednakże nasuwa się wątpliwość co do zidentyfikowania wszystkich celów przetwarzania danych odpowiadających kompetencjom i obowiązkom administratorów. Niejasność, nieprecyzyjność w zakresie określenia tychże celów przetwarzania danych może powodować problemy w toku konkretnego postępowania, w konkretnej jednostkowej sytuacji.

Kolejno w odniesieniu do art. 29a ust. 2 wskazać trzeba, że wątpliwości budzi wyłączenie przepisów art. 13 – 15 ust. 1 i 3, 18, 19 i 21 rozporządzenia 2016/679, generalnie w stosunku do przetwarzania danych osobowych przez administratorów danych, określonych w art. 29a ust. 1 projektu. Tu zastosowanie znajduje ogólna uwaga Generalnego Inspektora wskazana na początku załącznika a odnosząca się do wyłączeń stosowania rozporządzenia 2016/679 w zakresie praw podmiotów danych, niezgodnie z zasadami wynikającymi z art. 23 rozporządzenia. Projektodawca powinien nie tylko wykazać niezbędność ewentualnego ograniczenia tych praw, ale także jasno wskazać przyczynę wyłączenia oraz spełnić warunki, którym powinien odpowiadać akt prawny zawierający takie wyłączenia z art. 23 ust. 2 lit. a – h rozporządzenia 2016/679. Trudno tym samym dostrzec przyczynę generalnego zastosowania ww. wyłączeń. Nie wydaje się, aby przesłanką



takiego ewentualnego ograniczenia mogła być przesłanka z art. 23 ust. 1 pkt g rozporządzenia 2016/679. Oczywiście należy mieć na względzie zasady etyki przy wykonywaniu zawodu zaufania publicznego, ale ograniczenie uprawnień kontrolnych w każdej sytuacji, wzbudza poważne wątpliwości organu do spraw ochrony danych osobowych.

W odniesieniu do dodawanego art. 29a ust. 5 zwrócić uwagę należy na konieczność dookreślenia i doprecyzowania w tym przepisie jakie „procedury prawne dotyczące zabezpieczeń zapobiegającym nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu projektodawca” miał na myśli projektodawca, tj. jakie inne procedury prawne niż wynikające z rozporządzenia 2016/679. Zwrócić uwagę należy, że procedury zabezpieczeń zapobiegających nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu nie mogą ograniczać rozwiązań wynikających z rozporządzenia 2016/679.

W związku z zaproponowanym brzmieniem art. 29b projektu organ do spraw ochrony danych osobowych zgłasza zastrzeżenie do wyłączenia stosowania art. 58 ust. 1 lit. e i f rozporządzenia 2016/679. Osoby wykonujące ww. zawód nie są zwolnione z obowiązku przestrzegania przepisów o ochronie danych osobowych. Co więcej są one zobligowane do wprowadzenia odpowiednich środków ochrony danych osobowych adekwatnych do przetwarzanych danych. Wyłączenie stosowania art. 58 ust. 1 lit. e i f rozporządzenia 2016/679 ograniczy nie tylko możliwości kontrolne organu nadzorczego, ale również wykreuje obszary trwale wyłączone spod kontroli zgodności z prawem przetwarzania danych. Takie rozwiązania nie mogą być natomiast zaakceptowane przez Generalnego Inspektora Ochrony Danych Osobowych.

Projektodawca argumentuje wyłączenie ww. artykułu treścią art. 90 rozporządzenia 2016/679, a dokładnie ochroną tajemnicy zawodowej. Jednak nie należy utożsamiać ochrony ww. tajemnicy z uniemożliwieniem kontroli organu nadzorczego w zakresie zgodności przetwarzania danych z przepisami ogólnego rozporządzenia o ochronie danych. Przykładem tego typu sytuacji jest m.in. art. 3 ust. 1 pkt. 3 ustawy z dnia 6 lipca 1982 r. o radcach prawnych, który stanowi, iż *„Obowiązek zachowania tajemnicy zawodowej nie dotyczy informacji udostępnianych na podstawie przepisów ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2014 r. poz. 455 oraz z 2015 r. poz. 1223) - w zakresie określonym tymi przepisami.”* Reasumując istnieje obawa, że wyłączenie art. 58 ust. 1 lit. e i f rozporządzenia 2016/679 ograniczy możliwości kontrolne organu nadzorczego oraz może wykreować obszary trwale wyłączone spod kontroli zgodności z prawem przetwarzania danych.

Analizując dalej przepisy ww. ustaw należy zwrócić uwagę, że w opinii Generalnego Inspektora doprecyzowania wymaga kwestia przechowywania danych osobowych.

Zaproponowane przepisy w sposób lakoniczny i nieprecyzyjny regulują taki okres przechowywania danych, oddając ustalenie tego terminu administratorowi z uwzględnieniem celów przetwarzania i przepisów odrębnych dotyczących terminów. Zgodnie z motywem 39 rozporządzenia 2016/679 aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien zapewnić ograniczenia okresu przechowywania danych do ścisłego minimum, czyli ustalić termin ich usuwania lub okresowego przeglądu, co wynikać powinno z przedmiotowych przepisów wprost a nie bliżej nieokreślonych przepisów odrębnych.

#### **60. Zmiana ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570)**

W art. 73 projektu nie wprowadzono zmian w zakresie doprecyzowania wymagań dotyczących rozliczalności przetwarzanych danych w kontekście wymiany danych, o których mowa w art. 15 obecnej ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne<sup>15</sup>.

Zgodnie z wymaganiami art. 5 ust. 2 rozporządzenia 2016/679 administrator danych powinien być w stanie wykazać, że przetwarzane dane, w tym ich udostępnienie innym podmiotom jest adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane (art. 5 ust 1 litera c rozporządzenia 2016/679) Obecny przepis art. 15 ust 2 ww. ustawy oraz rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym<sup>16</sup>, rozliczalności takiej nie zapewnia, gdyż nie wymaga się, aby w przypadku żądania udostępnienia danych weryfikowana była rzeczywista potrzeba takiego udostępnienia, tj. np. udostępnienia danych dotyczących osoby X, tylko wtedy, gdy wykaże się, że określone dane potrzebne są do załatwienia sprawy zgłoszonej przez tę osobę. Ponadto obecnie obowiązujący wzór wniosku o udostępnienie informacji z rejestru publicznego stanowiący załącznik do ww. rozporządzenia jest mało precyzyjny i zezwala na bardzo szerokie udostępnienie przetwarzanych danych, a nie np. tylko do danych dotyczących wskazanej osoby.

Projektodawca powinien uzupełnić projekt w tym zakresie.

#### **61. Zmiana ustawy z dnia 30 czerwca 2005 r. o kinematografii (Dz. U z 2016 r. poz. 438 oraz z 2017 r. poz. 961)**

---

<sup>15</sup> Dz. U. z 2017 r. poz. 570 z późn. zm.

<sup>16</sup> Dz. U. z 2005 r. nr 205, poz. 1692 z późn. zm.

W art. 74 projektu projektodawca dodaje w ustawie o kinematografii Rozdział 4a zatytułowany „Ochrona danych osobowych”, do którego Generalny Inspektor zgłasza następujące uwagi.

Wątpliwości Generalnego Inspektora budzi przetwarzanie danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych (art. 30a ustawy o kinematografii) oraz danych o imionach rodziców danej osoby, jej dacie i miejscu urodzenia. Zasadne w tym miejscu są uwagi do art. 21 projektu.

Kolejną uwagę Generalny Inspektor kieruje do art. 30 ust. 5, który wskazuje 20-letni okres przechowywania danych osobowych, o których mowa w art. 8 ust. 1 pkt 6 i 7. W związku z zasadą ograniczenia przechowywania danych GODO podaje pod rozwagę projektodawcy czy taki okres przechowywania danych będzie adekwatny do realizacji celów administratorów. Jeżeli projektodawca uzna, że jest to konieczne to Generalny Inspektor sugeruje ustalenie okresowego przeglądu w celu oceny przydatności takich danych. Jednocześnie należy zauważyć, że projektodawca określa czas retencji danych tylko dla art. 30a ust. 2 pomijając przy tym dane osobowe, o których mowa w art. 30a ust. 1, 3 i 4. W związku z powyższym sugeruje się określenie czasu przechowywania danych osobowych w pozostałych przypadkach.

W odniesieniu do zastosowanych w art. 30b ust. 1 ograniczeń należy zauważyć, że nie wydaje się słuszne ograniczanie praw, o których mowa w art. 12, 15 rozporządzenia 2016/679 ze względu na interes finansowy państwa co uzasadnione jest szczegółowo w art. 21 projektu.

Przepis art. 30b ust. 2 ustanawia wyłączenie stosowania art. 14 rozporządzenia 2016/679 w celu zapewnienia prawidłowej realizacji zadań, o których mowa w art. 28 ust. 2 pkt 3,5 i 6. Analizując przepis art. 28 ust. 2 pkt 3,5 i 6 ustawy o kinematografii należy zauważyć, że zadania te związane są z archiwizacją materiałów dotyczących filmów i kinematografii a art. 28 ust. 5 głosi, że do działalności państwowej instytucji kultury wyspecjalizowanej w zakresie ochrony narodowego dziedzictwa kulturalnego w dziedzinie kinematografii i filmotek regionalnych w zakresie państwowego zasobu archiwalnego, określonej w ust. 2 pkt 1-3, stosuje się ustawę o narodowym zasobie archiwalnym i archiwach. W związku z powyższym takie wyłączenie jest nie celowe z punktu widzenia przepisów art. 89 rozporządzenia 2016/679 mówiącego o zabezpieczeniach i wyjątkach mających zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych

W art. 30b ust. 6 proponuje się także, aby podmioty wskazane w art. 30a- 30b mogły zlecać innym podmiotom przetwarzania danych osobowych na jego rzecz oraz pełnić funkcję podmiotu przetwarzającego dane na zlecenie innego podmiotu. Zastosowana konstrukcja jest niezgodna z

art. 28 rozporządzenia 2016/679, co wskazane zostało szczegółowo w uwagach do art. 21 projektu.

Projektowany art. 30b ust. 5 mówi, że dane osobowe, o których mowa w art. 30 a ust. 1-4, podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu i są przechowywane wyłącznie przez okres niezbędny do realizacji zadań, obowiązków i uprawnień (argumentacja z pkt 8 do art. 21 – zmiana ustawy o prawie autorskim i prawach pokrewnych).

Przepis art. 30b ust 3 również ogranicza stosowanie 34 rozporządzenia 2016/679. Zatem aktualna pozostaje argumentacja do art. 21 projektu odnosząca się do tej samej materii.

## **62. Zmiana ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2016 r. poz. 1318, z późn. zm.)**

Zadaniem organu do spraw ochrony danych osobowych wskazywanie projektodawcy zakresu, ewentualnie wymaganych w związku z rozpoczęciem stosowania w polskim porządku prawnym rozporządzenia unijnego, dostosowań przepisów ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego. Przedmiotowa ustawa obecnie reguluje problematykę przetwarzania danych osobowych przez te wojskowe służby specjalne, a art. 38 tej ustawy wprost odwołuje się do obowiązującej ustawy o ochronie danych osobowych, która ma utracić moc. Nie można przy tym pominąć, iż – zamieszczone w art. 38 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego – odwołanie do art. 28 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych jest błędne, albowiem odnosi się do brzmienia ustawy o ochronie danych osobowych nieobowiązującego od października 2001 roku.

Powstaje wszakże pytanie, na które odpowiedzieć musi projektodawca, czy celowe jest – zaproponowane w nowym brzmieniu art. 38 ust. 1a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego wyłączenie stosowania art. 13–22 rozporządzenia 2016/679 w odniesieniu do realizacji przez odpowiednie wojskowe służby specjalne zadań określonych w art. 5 ust. 1 i art. 6 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego. Kontrowersyjne jest bowiem, czy – przy uwzględnieniu brzmienia art. 2 ust. 2 rozporządzenia 2016/679 – do przetwarzania danych osobowych na potrzeby realizacji tych zadań rozporządzenie w ogóle znajduje zastosowanie. Dopiero odpowiedź na to pytanie, której projektodawca w uzasadnieniu nie udzielił, stanowić będzie podstawę analizy zasadności i zakresu zaproponowanego wyłączenia.

**63. Zmiana ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych (Dz. U. z 2016 r. poz. 758)**

Wątpliwości budzi odwołanie ujęte w art. 50a ust. 2 do art. 50 pkt 2-5, czyli w przepisie, który ma zostać uchylony. W odniesieniu do art. 54f należy ponownie zauważyć, iż niewystarczające i niegwarantujące zgodności z określonymi w rozporządzeniu 2016/679 zasadami dotyczącymi przetwarzania danych osobowych są – zamieszczone w omawianym przepisie – regulacje w przedmiocie udostępniania danych z centralnej ewidencji bezwnioskowo, w trybie pełnej teletransmisji danych. W szczególności przedstawiona propozycja uniemożliwia administratorowi realizację jednej z podstawowych zasad przetwarzania danych osobowych – zasady rozliczalności z art. 5 ust. 2 rozporządzenia 2016/679.

**64. Zmiana ustawy dnia 12 stycznia 2007 r. o drogowych spółkach specjalnego przeznaczenia (Dz. U. z 2015 r. poz. 1502 i 2260 oraz z 2016 r. poz. 2260)**

W art. 82 projektu (projektowany art. 4a ust. 1) ponownie użyto dotychczas stosowanej konstrukcji dającej spółce specjalnego przeznaczenia możliwość przetwarzania danych. Natomiast zgodnie z art. 6 ust. 1 lit. c rozporządzenia 2016/679 podstawą do przetwarzania może być jedynie obowiązek prawny ciążyący na administratorze. Obecna konstrukcja realizacji uprawnienia albo obowiązku wyrażona w art. 23 ust. 1 lit. b ustawy o ochronie danych osobowych nie będzie po 25 maja przyszłego roku dopuszczalna. Dlatego też konieczna jest zmiana brzmienia zaproponowanego przepisu.

Do art. 4a ust. 2 pkt 1 i 2, ust. 3, 4, 5-10 analogiczne zastosowanie mają uwagi zgłoszone do projektowanego art. 18 ust. 2b oraz ust. 2c-2j ustawy o drogach publicznych.

**65. Zmiana ustawy z dnia 15 czerwca 2007 r. o lekarzu sądowym (Dz.U. poz. 849, z 2008 r. poz. 293 i z 2011 r. poz. 622)**

W odniesieniu do art. 84 projektu - przepisów ustawy o lekarzu sądowym, wątpliwości wzbudza brzmienie art. 10a ust. 2 projektu, który przewiduje wyłączenie przepisów art. 13 – 15 ust. 1 i 3, 18, 19 i 21 rozporządzenia 2016/679, generalnie w stosunku do przetwarzania danych osobowych przez administratorów danych, określonych w art. 10a ust. 1 projektu. Tu zastosowanie znajdują ogólne uwagi Generalnego Inspektora do stosowania przez projektodawcę wyłączeń praw podmiotów danych niezgodnie z art. 23 rozporządzenia 2016/679.

W miejscu stwierdzić trzeba, że nie wydaje się, aby przesłanką takiego ograniczenia był art. 23 ust. 1 pkt f. Oczywiście należy mieć na względzie ochronę niezależności sądów i postępowania sądowego, ale ograniczenie uprawnień kontrolnych w każdej sytuacji i w odniesieniu do każdej osoby, której dane przetwarza lekarz sądowy, wzbudza poważne wątpliwości organu do spraw ochrony danych osobowych.

W odniesieniu do dodawanego art. 10a ust. 5 zwrócić uwagę należy na konieczność dookreślenia i doprecyzowania w tym przepisie jakie „procedury prawne dotyczące zabezpieczeń zapobiegającym nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu projektodawca” chce ustalić projektodawca, tj. jakie inne procedury prawne niż wynikające z rozporządzenia 2016/679. Zwrócić uwagę należy, że procedury zabezpieczeń zapobiegającym nadużyciom i niezgodnemu z prawem dostępowi lub przekazaniu nie mogą być wprowadzane wbrew zasadom i normom wynikającym z rozporządzenia 2016/679.

Ponadto, w opinii Generalnego Inspektora doprecyzowania wymaga kwestia przechowywania danych osobowych, zaproponowane przepisy tej ustawy w sposób lakoniczny i nieprecyzyjny regulują okres przechowywania danych, jako, że ustala ten termin administrator mając na uwadze cele przetwarzania. Zgodnie z motywem 39 rozporządzenia 2016/679 aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien zapewnić ograniczenia okresu przechowywania danych do ścisłego minimum, czyli ustalić termin ich usuwania lub okresowego przeglądu.

#### **66. Zmiana ustawy z dnia 15 czerwca 2007 r. o licencji doradcy restrukturyzacyjnego (Dz. U. z 2016 r. poz. 883)**

Zastrzeżenia organu do spraw ochrony danych osobowych budzi w art. 20a ust. 1 zmienianej ustawy brak wskazania zamkniętego katalogu danych osobowych przetwarzanych przez administratora danych (niezgodność z zasadą minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c rozporządzenia 2016/679)

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi art. 20a ust. 2 i 3 ustawy, zawierający wyłączenia art. 13-15 ust. 1 i 3, 18, 18 i 21 rozporządzenia 2016/679. Wprowadzanie ograniczeń w zakresie ww. przepisów rozporządzenia 2016/679, z pominięciem wskazania elementów określonych w art. 23 ust. 1 i 2 rozporządzenia 2016/679, oznacza niedopuszczalność wyłączenia przedmiotowych przepisów rozporządzenia 2016/679 (analogiczna uwaga do art. 2 i art. 21 przepisów wprowadzających). Art. 20a ust. 3 zmienianej ustawy stanowi, że wyłączenia stosuje się w przypadku danych osobowych niezbędnych do zapewnienia

prawidłowej realizacji zdań, natomiast projektodawca nie wskazując jakie dane mogą być uważane za niezbędne.

Wątpliwości GODO budzi art. 20a ust. 5 który w sposób bardzo ogólny stanowi o zabezpieczaniu danych osobowych, co jest niezgodne z zasadą rozliczalności określoną w art. 5 ust. 2 rozporządzenia 2016/679.

Zastrzeżenia Generalnego Inspektora budzi art. 20b stanowiący, że okres przechowywania danych osobowych ustala administrator zgodnie z celami ich przetwarzania. Powyższy przepis jest niezgodny z zasadą ograniczenia przechowywania określonym art. 5 ust. 1 pkt e. Uwaga GODO dotycząca obowiązującego już przepisu, zgłaszana była na etapie prac legislacyjnych i nieuwzględniona dotyczy art. 17 ust. 2 pkt 4 ustawy. Przepisy powszechnie obowiązującego prawa nie obligują osób fizycznych do posiadania telefonu, niezależnie od wykonywanego zawodu czy też podejmowanych zajęć. GODO jest przeciwny tworzeniu przepisów, które mocą powszechnie obowiązującego prawa nakładają na adresatów wymóg posiadania i podawania tego numeru dla potrzeb listy osób posiadających licencję doradcy restrukturyzacyjnego Zgodnie z treścią art. 17 ust. 3a ustawy imię i nazwisko oraz numer telefonu osoby posiadającej licencję doradcy restrukturyzacyjnego jest udostępniany w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Sprawiedliwości. Niezależnie od zastrzeżeń organu do spraw ochrony danych osobowych dotyczących braku wymogów ustawowych obligujących osobę fizyczną do posiadania numeru telefonu, organ wskazuje, że wszelkie informacje dotyczące danych takich osób powinny być opatrzone przymiotnikiem „służbowy” celem uniknięcia podawania prywatnego telefonu osób prowadzących tego rodzaju sprawy.

#### **67. Zmiana ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2017r. poz. 489, 624, 777, 952 i 1428)**

W odniesieniu do art. 86 projektu - w ustawie o pomocy osobom uprawnionym do alimentów, należy zgłosić uwagę do zaproponowanej zmiany brzmienia art. 15 ust. 8b ww. ustawy. Organ do spraw ochrony danych wskazuje, iż przepis ten zawiera odniesienie do przepisów o ochronie danych osobowych. Generalny Inspektor przypomina, iż przepisy o ochronie danych osobowych jako przepisy ogólne mają zastosowanie, niezależnie od odesłań znajdujących się w omawianych przepisach ustaw. Odesłania takie jak zaproponowane nie określają także w sposób wystarczający zasad przetwarzania danych przez ministra oraz upoważnione podmioty. To w tych przepisach szczególnych powinny być określone wyczerpująco zasady przetwarzania danych przez administratora oraz podmioty, którym udostępniane są dane, w szczególności tryb pozyskiwania,

udostępniania i przechowywania danych. Ogólne odesłanie do przepisów o ochronie danych osobowych może rodzić wątpliwości co do zasad przetwarzania danych mających zastosowanie.

Kolejno wątpliwości wzbudza ostatnie zdanie art. 15 ust. 8b, z przepisu tego bowiem nie wynika jakie dane osobowe i czyje dane będą przekazywane przez organ właściwy wierzyciela i organ właściwy dłużnika do rejestru centralnego. Takie uregulowanie kwestii udostępnienia danych jest nie do przyjęcia, bez określenia jakiegokolwiek zakresu udostępnianych danych, szczególnie pod kątem zasad wynikających z art. 5 RODO. Należy rozważyć kwestię ewentualnego współadministrowania danymi - wspólnego określania celów i sposobów przetwarzania, stosownie do zasad wynikających z art. 26 RODO.

#### **68. Zmiana ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318)**

Generalny Inspektor zwraca uwagę, że proponowane w art. 87 projektowanej ustawy brzmienie art. 47a ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta mówiące o tym, że Rzecznik może przetwarzać wszelkie informacje budzi wątpliwości z punktu widzenia zgodności z wynikającą z art. 51 ust. 2 Konstytucji zasadą adekwatności pozyskiwania, gromadzenia i udostępniania informacji o obywatelach oraz wyrażonej w art. 5 ust. 1 lit. c rozporządzenia 2016/679. Konieczne jest dookreślenie, w jakim zakresie i dla realizacji jakich celów Rzecznik Praw Pacjenta będzie mógł przetwarzać dane osobowe, przykładowo poprzez wskazanie, że Rzecznik przetwarza niezbędne do realizacji swoich ustawowych zadań.

Również posłużenie się w art. 47a ust. 1 ustawy wyrażeniem „może przetwarzać” nie spełnia wymagań wynikających z art. 51 ust. 2 Konstytucji oraz art. 5 ust. 1 lit. c rozporządzenia 2016/679 szerzej: uwagi do art. 15 projektu ustawy).

#### **69. Zmiana ustawy z dnia 7 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym (Dz. U. z 2016 r. poz. 1000 i 1948)**

Należy zwrócić uwagę, że ww. ustawa straciła moc i zastąpiona została przez ustawę z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2017 r. poz. 1089). Projektodawca powinien zweryfikować, czy zaproponowane zmiany są prawidłowe, czy i jakie znaczenie mają wobec przepisów nowej ustawy w tym zakresie oraz czy są wystarczające do dostosowania przepisów do RODO. Pomocne w tym zakresie mogą być uwagi GIODO zgłaszane w trakcie prac legislacyjnych w poprzednich latach.



**70. Zmiana ustawy z dnia 9 października 2009 r. o dyscyplinie wojskowej (Dz. U. z 2016 r. poz. 772 i 2138)**

Odnosząc się do art. 94 projektu ustawy, w opinii Generalnego Inspektora Ochrony Danych Osobowych, brak jest uzasadnienia do wyłączenia stosowania przepisów art. 12 ust. 3 i 4, art. 13, 14, 17-22, 34 rozporządzenia 2016/679. Uwagi poczynione wyżej (uwagi do art.2) w tym zakresie mają odpowiednie zastosowanie.

**71. Zmiana ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo kredytowych (Dz. U. z 2016 r. poz. 1910, z późn. zm.)**

Zastrzeżenia GIODO budzi art. 16b, stanowiący, że do działalności kas stosuje się m.in. art. 112b ust. 1 i art. 112e ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe – uwaga ta jest tożsama z uwagą Generalnego Inspektora wniesioną do art. 41 projektu (ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe), w zakresie art. 112b ust. 1 i art. 112e.

**72. Zmiana ustawy z dnia 19 listopada 2009 r. o grach hazardowych (Dz.U. z 2016 r. poz. 471, 1948 i 2260 oraz z 2017 r. poz. 88 i 1089)**

W art. 96 pkt 2 projektu zaproponowano uregulowanie przetwarzania przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego danych w związku z prowadzeniem Funduszu Promocji Kultury. W projektowanym ust. 6a należy usunąć określenie „w szczególności”, które tworzy otwarty katalog danych osobowych. Wśród zaproponowanych danych za zbędne należy uznać przetwarzania daty i miejsca urodzenia oraz imion rodziców (lit. d i f), gdyż jednocześnie przetwarzany jest identyfikator podatkowy (lit. e). W lit. h proponuje się dodanie wyrażenia „o ile zostanie podany”, gdyż obecnie nie istnieje obowiązek posiadania numeru telefonu i adresu poczty elektronicznej.

Dodatkowo należy zauważyć, iż niejasne są cele przetwarzania danych ujęte w komentowanych ustępach. W art. 87 ustawy z dnia 19 listopada 2009 r. o grach hazardowych<sup>17</sup> uregulowane istnienie w/w funduszu, w tym ogólnie wskazano jego zadanie jako promowanie lub wspieranie m.in. przedsięwzięć artystycznych, twórczości, ochrony polskiego dziedzictwa narodowego, spłaty wieloletnich zobowiązań finansowych instytucji kultury. Tym samym nie jest jasne, dla jakich zadań niezbędne jest przetwarzanie danych ujętych w pkt 2 projektowanego ust.

---

<sup>17</sup> Dz. U. z 2016 r. poz. 471 z późn. zm., dalej zwana ustawą o grach.

6a. Także do tego przepisu należy podnieść uwagę poczynioną wyżej, dotyczącą numeru telefonu i adresu poczty elektronicznej.

Niemożliwym jest odniesienie się do zaprojektowanych w ust. 6b okresów retencji danych, gdyż uzasadnienie nie zawiera żadnego wyjaśnienia w tym zakresie. Dla oceny zasadności przyjęcia takich okresów konieczne jest ich umotywowanie, właściwe uzasadnienie. W związku z powyższym w sprzeczności stoi projektowany ust. 6d, w którym wskazano, że dane są przechowywane wyłącznie przez okres niezbędny do realizacji zadań, obowiązków i uprawnień. W zakresie w jakim przepis ten nie tworzy szczególnych zasad zabezpieczenia danych jest on zbędny z punktu widzenia przepisów RODO.

Zaproponowane w ust. 6e-6h ograniczenia praw osób, których dane dotyczą należy uznać za niezgodne z art. 23 RODO. Uzasadnienie tych propozycji wskazuje na chęć zapewnienia wygody administratorowi przetwarzanych w związku z funkcjonowaniem w/w funduszu. Nie można uznać, by powody te spełniały przesłanki i wymogi określone w art. 23 RODO.

W opinii organu ds. ochrony danych osobowych należy zweryfikować, czy proponowane zmiany są jedynymi, które należy przeprowadzić w przepisach ustawy o grach. Wyczerpującego uregulowania w przepisach ustawowych wymaga chociażby kwestia monitoringu wizyjnego ujęta w art. 15ba ustawy o grach. Na kwestię tę zwracano uwagę w ostatnim czasie Ministrowi Finansów.<sup>18</sup>

### **73. Zmiana ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2017 r. poz. 1464)**

Generalny Inspektor Ochrony Danych Osobowych stoi na stanowisku, że projektodawca powinien dokonać analizy zasadności i zakresu, zawnioskowanego w art. 9a ust. 2 ustawy o dowodach osobistych, wyłączenia stosowania art. 16, art. 18 i art. 21 rozporządzenia 2016/679. Z brzmienia komentowanego przepisu nie wynika bowiem cel zastosowania przedmiotowego wyłączenia ani przyczyna, dla której zostało ono zaproponowane. Przypomnieć zaś wypada, iż prawodawca unijny umożliwił wprowadzenie ograniczeń niektórych praw i obowiązków przewidzianych w rozporządzeniu unijnym wyłącznie w przypadku, gdy proponujący takie ograniczenie wykaże, że jest ono niezbędne i proporcjonalne w demokratycznym społeczeństwie ze względu na wartości wskazane w art. 23 ust. 1 rozporządzenia 2016/679. Tymczasem w art. 9a ust. 2 ustawy o dowodach osobistych porzeczano jedynie na stwierdzeniu, iż: „przetwarzanie danych osobowych następuje z wyłączeniem art. 16, 18 i 21 rozporządzenia...”, nie odnosząc się w

---

<sup>18</sup> Sygn. DOLiS-023-348/17/KK/61592, 69811 z dnia 9 sierpnia 2017 r.,  
<http://legislacja.rcl.gov.pl/projekt/12300900/katalog/12449202#12449202>

żaden sposób do – wyżej zaprezentowanych – kwestii podniesionych w art. 23 ust. 1 rozporządzenia 2016/679.

Na brak dokonania przez projektodawcę – sugerowanej przez organ do spraw ochrony danych osobowych – analizy zasadności ustanowienia wnioskowanych wyłączeń wskazuje choćby fakt, że wśród przewidzianych do wyłączenia przepisów rozporządzenia unijnego znajduje się też art. 21 tego rozporządzenia, który to przepis w ogóle nie znajduje zastosowania do przetwarzania danych osobowych w zakresie określonym w ustawie o dowodach osobistych.

Niezależnie od powyższego Generalny Inspektor Ochrony Danych Osobowych po raz kolejny sygnalizuje, że niewystarczające i niegwarantujące zgodności z określonymi w rozporządzeniu unijnym zasadami dotyczącymi przetwarzania danych osobowych są – zamieszczone w art. 66 ustawy o dowodach osobistych – regulacje w przedmiocie udostępniania danych z Rejestru Dowodów Osobistych bezwnioskowo, w trybie się pełnej teletransmisji danych. W szczególności obowiązujące brzmienie art. 66 ustawy o dowodach osobistych uniemożliwia administratorowi realizację jednej z podstawowych zasad przetwarzania danych osobowych – zasady rozliczalności z art. 5 ust. 2 rozporządzenia 2016/679.

#### **74. Zmiana ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2017 r. poz. 657)**

Do art. 5a ust. 2 ustawy o ewidencji ludności, Generalny Inspektor Ochrony Danych Osobowych zgłasza analogiczną uwagę co do zamieszczonej w opinii do art. 9a ust. 2 ustawy o dowodach osobistych.

Zachowuje pełną aktualność w odniesieniu do art. 48 ustawy o ewidencji ludności dotyczącego udostępniania danych z rejestru PESEL za pomocą urządzeń teletransmisji danych (po złożeniu jednorazowego, uproszczonego wniosku) kierunkowa uwaga Generalnego Inspektora Ochrony Danych Osobowych do art. 66 ustawy o dowodach osobistych. Problem ten był już podnoszony przez organ do spraw ochrony danych osobowych w postępowaniu administracyjnym w przedmiocie pozyskiwania przez komorników sądowych danych przetwarzanych w rejestrze PESEL.

W szczególności obowiązujące brzmienie art. art. 48 ustawy o ewidencji ludności uniemożliwia administratorowi realizację jednej z podstawowych zasad przetwarzania danych osobowych – zasady rozliczalności z art. 5 ust. 2 rozporządzenia 2016/679.

W ramach uwag do projektowanego art. 101 należy zauważyć, iż przepisy o ochronie danych osobowych – ustawa o ochronie danych osobowych czy RODO – nie regulują udostępniania na wniosek wykazów danych tworzonych przez ich administratorów. Dlatego też regulacja projektowana w art. 143 paragraf 4 ustawy Kodeks wyborczy powinna być przedmiotem przepisów szczególnych, powinny one regulować szczegółowo tryb i zasady udostępniania do wglądu na wniosek przedmiotowego „wykazu wpłat obywateli polskich na rzecz komitetu wyborczego organizacji i komitetu wyborczego wyborców” dokonywanego przez Państwową Komisję Wyborczą, jak i przez komisarza wyborczego.

#### **75. Zmiana ustawy z dnia 25 marca 2011 r. o Centrum Polsko-Rosyjskiego Dialogu i Porozumienia (Dz. U. z 2016 r., poz. 494)**

Odnosząc się do projektowanego art. 24 ust. 3 zmienianej ustawy uzasadnienia wymaga tak długi okres retencji danych.

Wątpliwości Generalnego Inspektora budzi również przewidziany w art. 24 ust. 5 okres przechowywania danych osobowych zawartych we wniosku o uzyskanie stypendium oraz w art. 25 ust. 7 okres przechowywania danych osobowych zawartych we wniosku o udzielenie dofinansowania przedsięwzięcia. Niezbędnym jest wyjaśnienie, czy z punktu widzenia zasady ograniczenia przechowywania wyrażonej w art. 5 ust. 1 lit d Rozporządzenia nr 2016/679 przewidziany w tych przepisach 20 letni okres przechowywania danych jest niezbędny do realizacji celów, w których dane te są przetwarzane.

Zwrócić również należy uwagę, iż pozyskiwanie numeru telefonu oraz adresu poczty elektronicznej nie może być obowiązkowe, lecz dobrowolne (art. 24 ust. 3 pkt 8, art. 25 ust. 3 pkt 1 lit. g).

Generalny Inspektor zwraca uwagę na wątpliwości wobec art. 27a, który ma być dodany po art. 27. W ocenie Generalnego Inspektora dodawany do ustawy art. 27a ust. 1 ma zbyt ogólny charakter. Konstrukcja tego przepisu pozwala na bardzo szeroką interpretację, co może prowadzić do pozyskiwania danych osobowych w szerszym zakresie, niż jest to niezbędne przez wskazane w przepisie podmioty. Przepis ten daje bowiem możliwość przetwarzania danych osobowych nieskonkretyzowanych osób, w bardzo szerokim zakresie w celach bardzo szeroko ujętych (realizacja zadań o których mowa w art. 3 ust. 2, art. 8 ust. 1, art. 10 ust. 1 i 3, art. 11, art. 12 ust. 2, art. 13, art. 16, art. 17 ust. 1, art. 18 ust. 1, art. 21 ust. 2, art. 24 ust. 1, art. 25, art. 26 ust. 1-3, art. 27 oraz art. 28). W art. 27a ust. 2 konieczne jest doprecyzowanie – w jakich sytuacjach, w jakich celach – ma dochodzić do powierzania przetwarzania danych osobowych.

Generalny Inspektor wskazuje, w przewidzianym w **art. 102 pkt 4** projektu ustawy wyłączenie stosowania art. 13 i art. 19 rozporządzenia nr 2016/679 w **art. 27a ust. 5** ustawy nie przewidziano przepisów szczególnych czyniących zadość wszystkim wymaganiom określonym w art. 23 ust. 2 rozporządzenia nr 2016/679 (zob. szerzej: uwagi do art. 2 oraz art. 21 projektu ustawy).

#### **76. Zmiana ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2016 r. poz. 1927 i 1984).**

Należy zauważyć, iż zaproponowana nowelizacja ustawy dotyczy wyłącznie szkół artystycznych i placówek prowadzonych lub nadzorowanych przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego. Taka regulacja wydaje się niepełna, zatem Generalny Inspektor wskazuje na potrzebę dokonania przez projektodawcę dodatkowej analizy w tym zakresie. Niezależnie od powyższego, zastrzeżenia organu wzbudzają następujące kwestie.

Biorąc pod uwagę zasadę minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c RODO sugeruje się stworzenie zamkniętych katalogów danych, poprzez usunięcie sformułowania „w szczególności” (*vide* proponowane brzmienie art. 116a ust. 1).

Nie jest zrozumiałe generalnie uprawnienie do przetwarzania takich danych jak: wykształcenie, miejsce pracy i zajmowane stanowisko, w tym wysokość wynagrodzenia oraz numer rachunku bankowego. Niewątpliwie w indywidualnych przypadkach pozyskiwanie takich danych może być uzasadnione, jednak przepisy powinny takie okoliczności wskazywać, zamiast tworzyć ogólny przepis pozwalający na przetwarzanie tak szczegółowych informacji.

Jednocześnie w przypadku przetwarzania danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych – mając na uwadze, że w polskim porządku prawnym nie istnieje obowiązek posiadania przez osoby fizyczne takich środków komunikacji – należy pozostawić swobodę możliwości podawania takich danych.

Wątpliwości Generalnego Inspektora wzbudzają zaproponowane przez projektodawcę szerokie wyłączenia od stosowania przepisów RODO, polegające na odstąpieniu od stosowania art. 13, art. 14 oraz art. 17-19 RODO w zakresie, w jakim dane są niezbędne do zapewnienie realizacji zadań, o których mowa w ustawie oraz odstąpieniu od stosowania art. 5 ust. 2 RODO – w zakresie obowiązków wykazywania przestrzegania przepisów art. 5 ust. 1 rozporządzenia. Ponadto projektodawca zdecydował, aby wyłączyć stosowanie art. 34 RODO, w przypadku, gdy administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda

komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej. Ograniczone zostało również stosowanie art. 12 oraz art. 15 RODO.

Wyłączenia powyższe wymagają ponownej weryfikacji i ewentualnego dalszego doprecyzowania, w świetle argumentów przedstawionych powyżej odnośnie do art. 2, art. 21 oraz art. 28 przepisów wprowadzających.

Odnosząc się do projektowanego art. 116a ust. 6 ustawy o systemie informacji oświatowej, GİODO zauważa, iż okres retencji danych sformułowany został w sposób nieprecyzyjny, stanowi bowiem w istocie powtórzenie zasady ogólnej, sugeruje się zatem jego dookreślenie.

Art. 116a ust. 8 zakłada możliwość zlecania przetwarzania danych osobowych lub pełnienie funkcji podmiotu przetwarzającego te dane osobowe na zlecenie innego podmiotu przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego, specjalistyczną jednostkę nadzoru, dyrektora szkoły artystycznej lub placówki prowadzonej lub nadzorowanej przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego. Z uwagi na zbyt ogółe i nieostre sformułowanie tej propozycji przepisu, powtórzenia wymagają uwagi wyrażone powyżej w odniesieniu do art. 21 projektu.

## **77. Zmiana ustawy z dnia 11 maja 2011 r. o Krajowej Radzie Sądownictwa (Dz. U. z 2016 r., poz. 976 ze zm.)**

Generalny Inspektor zwraca uwagę na treść art. 106 projektu ustawy, który przewiduje dodanie nowej kompetencji Krajowej Rady Sądownictwa polegającej na sprawowaniu nadzoru nad przetwarzaniem danych osobowych przez Trybunał Konstytucyjny, Naczelny Sąd Administracyjny, Sąd Najwyższy oraz sądy apelacyjne, w ramach prowadzonych przez te organy postępowań oraz przewidziane w projekcie ustawy zmiany w przepisach regulujących organizację poszczególnych sądów (art. 52 projektu ustawy zmieniający ustawę z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, Dz. U. z 2016 r., poz. 2062 ze zm., dalej: p.u.s.p.<sup>19</sup>, art. 58 projektu ustawy zmieniający ustawę z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych, Dz. U. z 2016 r. poz. 1066 i 2261, art. 59 projektu ustawy zmieniający ustawę z dnia 23 listopada 2002 r. o Sądzie Najwyższym, Dz. U. z 2016 r. poz. 1254 ze zm., art. 35 projektu ustawy zmieniający ustawę z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych, Dz. U. z 2016 r. poz. 358ze zm.) oraz Trybunału Konstytucyjnego (art. 131 projektu ustawy zmieniający ustawę z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym, Dz. U. poz. 2072).

---

<sup>19</sup> Zob. stanowiska GİODO wyrażone w opiniach: DOLiS-033-23/14, DOLiS-072-10/15, DOLiS-033-604/12/AFS.

Rozporządzenie nr 2016/679 w art. 55 ust. 3 w sposób wyraźny wyłącza właściwość organów nadzorczych w kwestii nadzorowania operacji przetwarzania danych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości. W motywie 20 wyjaśniono, że wyłączenie właściwości organu nadzorczego nad sprawowaniem wymiaru sprawiedliwości przez sądy ma służyć ochronie niezawisłości sprawowania wymiaru sprawiedliwości. W treści tego motywu wskazano również, że konieczne jest zapewnienie możliwości powierzenia nadzoru nad takimi operacjami przetwarzania danych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego, organy te powinny w szczególności zapewnić przestrzeganie przepisów niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takimi operacjami przetwarzania danych. Sytuacja, w której to organ należący do systemu wymiaru sprawiedliwości ocenia spełnienie przesłanki niezbędności do ustalenia, dochodzenia lub obrony roszczeń w ramach sprawowania wymiaru sprawiedliwości przez sądy niewątpliwie służy zapewnieniu niezawisłości sprawowania wymiaru sprawiedliwości, o której mowa w motywie 20 rozporządzenia nr 2016/679.

Z tego punktu widzenia w pierwszej kolejności należy ocenić, czy Krajowa Rada Sądownictwa może być uznana za „specjalny organ w systemie wymiaru sprawiedliwości państwa członkowskiego”, o którym mowa w motywie 20 rozporządzenia nr 2016/679. Zgodnie z utrwaloną linią orzecniczą Trybunału Konstytucyjnego, Krajowa Rada Sądownictwa jest konstytucyjnym, kolegiальnym organem państwa, a jej zadania statuuja ją w bezpośredniej bliskości władzy sądowniczej, co wynika z systematyki Konstytucji, konstytucyjnie określonego składu Rady i jej kompetencji (zob. przykładowo: wyrok TK z 18 lipca 2007 r., sygn. akt K 25/07, OTK ZU nr 7/A/2007, poz. 80, wyrok TK z 16 kwietnia 2008 r., sygn. akt K 40/07, OTK ZU nr ). Jednak z uwagi na wynikający z art. 187 ust. 1 Konstytucji mieszany charakter składu KRS – łączy przedstawicieli środowiska sędziowskiego (z obligatoryjnym udziałem Prezesów SN i NSA), przedstawicieli władzy wykonawczej (Ministra Sprawiedliwości i osoby powołanej przez Prezydenta RP) oraz władzy wykonawczej (4 posłów i 2 senatorów) – nie sposób uznać, że organ ten jest organem władzy sądowniczej, a tym bardziej, że stanowi organ funkcjonujący w systemie wymiaru sprawiedliwości.

Generalny Inspektor nie jest właściwy do wskazywania, czy „specjalne organy w systemie wymiaru sprawiedliwości”, o których mowa w motywie 20 rozporządzenia nr 2016/679 powinny być nowo utworzonymi organami funkcjonującymi w ramach sądów sprawujących wymiar sprawiedliwości, czy też kompetencje te powinny być przyznane organom już istniejącym. Jednak w ocenie Generalnego Inspektora, z uwagi na określony w art. 187 ust. 1 Konstytucji skład KRS, a

mianowicie funkcjonowanie w KRS przedstawicieli władzy wykonawczej oraz władzy ustawodawczej, wątpliwości budzi, czy powierzenie nadzoru nad przetwarzaniem danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości temu organowi będzie służyć celowi określonemu w motywie 20 rozporządzenia nr 2016/679, czyli ochronie niezawisłości sprawowania wymiaru sprawiedliwości przez sądy. Art. 52 pkt 6 projektu ustawy stanowi m.in., że nadzór nad przetwarzaniem danych osobowych w ramach systemów teleinformatycznych oraz w postępowaniach sądowych przez sądy rejonowe ma sprawować prezes sądu okręgowego, a przez sądy okręgowe – prezes sądu apelacyjnego. W świetle obecnego brzmienia art. 23-25 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2016 r., poz. 2062 ze zm.) zasadnym jest rozważenie, czy w sytuacji w której prezesi tych sądów wybierani są przez Ministra Sprawiedliwości bez prawa wiążącego sprzeciwu, istotnie są właściwymi organami do sprawowania nadzoru nad przetwarzaniem danych przez sądy sprawujące wymiar sprawiedliwości.

Nie budzi natomiast wątpliwości Generalnego Inspektora wprowadzenie w ramach sądownictwa administracyjnego rozwiązania przewidzianego w art. 58 pkt 2 projektu ustawy, zgodnie z którym Prezes Naczelnego Sądu Administracyjnego sprawuje nadzór nad przetwarzaniem danych osobowych przez wojewódzkie sądy administracyjne w postępowaniach sądowych. Wprowadzenie takiego samego rozwiązania ustanawiającego nadzór prezesa wojskowego sądu okręgowego nad przetwarzaniem danych osobowych w postępowaniach przez wojskowe sądy administracyjne przewiduje art. 35 projektu ustawy.

Generalny Inspektor zwraca również uwagę na konieczność rozważenia, czy nie byłoby zasadnym uregulowanie sposobu prowadzenia postępowania oraz praw stron w związku ze sprawowaniem nadzoru przez specjalne organy w systemie wymiaru sprawiedliwości nad przetwarzaniem danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości. Regulacja przewidziana w art. 175g § 2 p.u.s.p. wydaje się nie określać wszystkich istotnych elementów związanych ze sprawowaniem tego nadzoru, w szczególności z prowadzonymi postępowaniami przed tym organem.

Z kolei przewidziane w **art. 106** oraz w **art. 131** projektu ustawy objęcie nadzorem Krajowej Rady Sądownictwa przetwarzania danych osobowych przez Trybunał Konstytucyjny w ramach prowadzonych przez niego postępowań budzi wątpliwości z uwagi na to, że Trybunał Konstytucyjny nie jest sądem w rozumieniu art. 175 Konstytucji oraz nie sprawuje wymiaru sprawiedliwości. W polskim porządku występują dwa rodzaje organów władzy sądowniczej: sądy i trybunały (zob. art. 10 ust. 2 oraz art. 173 Konstytucji). Jak wskazano powyżej, zgodnie z art. 175



Konstytucji wymiar sprawiedliwości w Rzeczypospolitej Polskiej sprawują Sąd Najwyższy, sądy powszechne, sądy administracyjne oraz sądy wojskowe. Kompetencje Trybunału Konstytucyjnego zostały określone w art. 188 Konstytucji i są związane z badaniem hierarchicznej zgodności aktów normatywnych w polskim systemie prawnym, nie zaś ze sprawowaniem wymiaru sprawiedliwości. Należy zauważyć, że art. 55 ust. 3 rozporządzenia nr 2016/679 wyraźnie przewiduje brak właściwości organu nadzorczego w zakresie nadzorowania operacji przetwarzania danych dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości. Z uwagi na to, że Trybunał Konstytucyjny nie sprawuje wymiaru sprawiedliwości nie sposób przyjąć, że przetwarzanie danych osobowych przez ten organ jest wyłączone z zakresu właściwości organu nadzorczego. Z tej przyczyny Generalny Inspektor sygnalizuje konieczność rozważenia, czy przewidziane w **art. 106 oraz art. 131 projektu** ustawy rozwiązanie przewidujące nadzór Krajowej Rady Sądownictwa nad przetwarzaniem danych osobowych w ramach postępowania przed Trybunałem Konstytucyjnym czyni zadość postanowieniom art. 55 ust. 3 oraz motywu 20 rozporządzenia nr 2016/679.

#### **78. Zmiana ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. z 2016 r. poz. 1572 i 1997 oraz z 2017 r. poz. 1089)**

W art. 111 projektu zaproponowano – nowe brzmienie art. 10 ust. 1 ww. ustawy – wyłączenie możliwości przetwarzania szczególnych kategorii danych, o których mowa w art. 9 RODO. W obecnym stanie prawnym wyłączenie to obejmuje dane ujęte w art. 27 ustawy o ochronie danych osobowych, w tym także dane dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Brak odniesienia projektodawcy do art. 10 RODO oznaczać może, iż dostawcy i podmioty prowadzące systemy płatności będą mogły przetwarzać dane dotyczące wyroków skazujących i naruszeń prawa. O ile w projektowanym art. 10a wskazano zasady dopuszczalności takich danych pracownika i osoby ubiegającej się o zatrudnienie, to nie ma wprowadzono zakazu przetwarzania takich danych o wszystkich innych osobach, w tym klientach. Takie rozwiązanie należy uznać za niedopuszczalne. Zgodnie z art. 10 RODO takiego przetwarzania wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Zgodnie z nowym brzmieniem art. 10 ust. 2 dopuszczalnym miałyby być przetwarzania danych zawartych w dokumentach tożsamości oraz danych biometrycznych. Projektodawca

powinien doprecyzować, jakie konkretnie dane z dowodów osobistych oraz dane biometryczne powinny być przetwarzane w celach niezbędnych do potwierdzania tożsamości osoby oraz wykazać niezbędność przyjmowanych rozwiązań. Byłoby to zgodne z zasadą minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c RODO oraz art. 6 ust. 1 lit. b RODO. W zakresie danych biometrycznych konieczne jest także przeprowadzenie analizy oceny skutków dla ochrony danych zgodnie z art. 35 ust. 3 lit. c oraz ust. 7 RODO.

W nowym art. 10a zaproponowano możliwość weryfikacji karalności pracowników i osób ubiegających się o zatrudnienie na stanowisku umożliwiającym dostęp do danych. Projektodawca powinien mieć świadomość, iż równolegle Ministerstwo Rozwoju prowadzi prace legislacyjne mające wprowadzić takie rozwiązanie na szerszą skalę – w projekcie ustawy o zasadach badania niekaralności kandydatów ubiegających się o zatrudnienie w podmiotach sektora finansowego. Aktualne pozostaje negatywne stanowisko Generalnego Inspektora wyrażone wobec powyższego projektu w dniu 14 września br<sup>20</sup>. Projektodawca powinien je wziąć pod uwagę w obecnym procesie legislacyjnym.

W nowym art. 10b zaproponowano ograniczenie następujących uprawnień osoby, której dane dotyczą:

- 1) uzyskanie informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu w zakresie niezbędnym do przeciwdziałania oszustwom, prowadzenia systemu płatniczego oraz dochodzenia i wykrywania oszustw (art. 13 ust. 2 lit. f, art. 14 ust. 2 lit. g i art. 15 ust. 1 lit. h),
- 2) zawiadomienie o naruszeniu ochrony jej danych;
- 3) udzielania informacji i prowadzenia komunikacji nie częściej niż raz na 3 miesiące;
- 4) prawa do przenoszenia danych;
- 5) prawa do bycia zapomnianym.

Podając podstawy do całkowitego wyłączenia tych praw wskazano kilka z nich, które jednak nie są adekwatne do omawianych przypadków. Wątpliwość budzi podawanie zapewnienia bezpieczeństwa publicznego (lit. c), innych ważnych celów (...) w tym kwestii pieniężnych, budżetowych i podatkowych (...) (lit. e) – w zakresie niesprecyzowania tego celu, ochrony osoby, której dane dotyczą (lit. i). Projektodawca zauważył jedynie, że na uwagę zasługują w/w cele, jednak nie wskazał, dlaczego miałyby one uzasadniać ograniczenie praw. W związku z powyższym należy stwierdzić, iż nie spełniają one wymogów z art. 23 RODO. Całkowite wyłączenie w/w praw

---

<sup>20</sup> Sygn. DOLiS-023-399/17/KK/69453 z dnia 14 września 2017 r.,  
<http://legislacja.rcl.gov.pl/docs/2/12302300/12455164/12455167/dokument310818.pdf>

należy uznać za wykraczające poza dyspozycję art. 23 ust. 1 RODO, które pozwala na wprowadzenie ograniczeń, które nie będą naruszać istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym. Zaproponowane regulacje nie wypełniają także wymogów ujętych w art. 23 ust. 2, który zawiera szeroki katalog przepisów, które powinny być przyjęte. Dodatkowo ta szeroka grupa wyłączeń nie została w sposób wystarczający uzasadniona (wymieniono przykładowe cele i zakres wyłączeń) ani nie dokonano oceny skutków dla ochrony danych zgodnie z art. 35 RODO, która jest obowiązkowa w przypadku zautomatyzowanego podejmowania decyzji.

#### **79. Zmiana ustawy z dnia 19 sierpnia 2011 r. o weteranach działań poza granicami państwa (Dz. U. poz. 1203 i z 2017 r. poz. 60)**

Projektodawca w art. 112 projektu dodaje art. 38a i dokonuje następujących wyłączeń stosowania przepisów RODO tj. obowiązków informacyjnych (art. 12 ust. 3 i 4, art. 13, art. 14), prawa usunięcia danych (art. 17), ograniczenia przetwarzania (art. 18), obowiązku poinformowania o usunięciu i ograniczeniu (art. 19), przenoszenia danych (art. 20), sprzeciwu (art. 21), automatyczne podejmowanie decyzji (art. 22), obowiązku zawiadamiania osoby o naruszeniu ochrony jej danych osobowych (art. 34) w odniesieniu do przetwarzania danych, o których mowa w: art. 7 (przyznanie statusu weterana – wnioski i zaświadczenia), art. 8 (dokumenty będące podstawą do ubiegania się o przyznanie statusu weterana), art. 9 (legitymacja weterana jako dokument potwierdzający status weterana oraz weterana poszkodowanego), art. 10 (rozporządzenie dotyczące wzoru zaświadczenia art. 7 ust. 1 pkt 2 i legitymacji), art. 26 (prawo do uzyskania pomocy finansowej przez weterana poszkodowanego-żołnierza na jedną z wymienionych form kształcenia), art. 31 (przyznawanie zapomogi dla Weterana-żołnierza, który ukończył 65 lat życia, lub weterana poszkodowanego-żołnierza) ustawy o weteranach działań poza granicami państwa.

W opinii GODO w przepisie art. 38a nie został wprost wskazany cel wyłączenia art. 12 ust. 3 i 4, art. 13, art. 14, art. 17 – 22 i art. 34 RODO. Projektodawca stosując wyłączenia z art. 23 ust. 1 lit. a – j RODO powinien spełnić jedną z enumeratywnie wymienionych w tym przepisie przesłanek. Co więcej jeżeli projektodawca widzi potrzebę wyłączenia art. 12 ust. 3 i 4, art. 13, art. 14, art. 17 – 22 i art. 34 RODO to powinien nie tylko jasno wskazać przyczynę wyłączenia lecz również spełnić warunki, którym powinien odpowiadać akt prawny zawierający takie wyłączenia z art. 23 ust. 2 lit. a – h RODO.

GIODO wskazuje, że nie zasadne wydaje się wyłączenie praw weteranów zagwarantowanych im w przepisach RODO w odniesieniu do przetwarzania ich danych wskazanych w przepisach art. 7-10, art. 26 i art. 31 ustawy o weteranach działań poza granicami państwa. Brak celu wyłączenia we wskazanym przepisie oraz brak informacji w uzasadnieniu do projektu o przyczynach takiej regulacji nie pozwala Generalnemu Inspektorowi na merytoryczną ocenę zaproponowanego w art. 38a rozwiązania. Jednocześnie takie wyłączenie w opinii organu do spraw ochrony danych osobowych nie znajduje uzasadnienia w przesłankach z art. 23 ust. 1 lit. a-j.

**80. Zmiana ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2016 r. poz. 1113, 1250, 1823 i 1948 oraz z 2017 r. poz. 1128)**

W art. 113 projektu ze zdziwieniem należy przyjąć propozycję dodania art. 9 ust. 4a, który zawiera obowiązek dołączenia oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych. Jest to zbędne z uwagi na treść art. 9 ust. 1 komentowanej ustawy, w którym określono obowiązki osoby chcącej prowadzić pocztową działalność regulowaną. Generalny Inspektor po raz kolejny przypomina, iż obecna propozycja, wielokrotnie już krytykowana w wielu projektach, przeczy idei zgody jako podstawy przetwarzania danych, zdefiniowanej w art. 7 RODO.

W odniesieniu do zaproponowanego okresu retencji danych, należy zauważyć, iż wykonywanie działalności oraz realizacja zadań i obowiązków ustawowych Prezesa UKE może trwać dłużej niż 10 lat od daty otrzymania danych. W uzasadnieniu słusznie wskazano, że dane operatora są wykreślane z rejestru z chwilą zaprzestania działalności np. ze względu na obowiązki sprawozdawcze. Obecne brzmienie przepisu utrudni wykonywanie tych zadań operatorowi, jak i Prezesowi UKE. Projektodawca powinien przeformułować brzmienie przepisu i wskazać sztywny okres przechowywania danych, który będzie odpowiadał zadaniom stawianym Prezesowi Urzędu oraz operatorowi. Zaproponowany czas przechowywania powinien odpowiadać zasadzie ograniczenia przechowywania ujętej w art. 5 ust. 1 lit. e RODO.

**81. Zmiana ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności (Dz. U. z 2016 r. poz. 217, 1579 i 1948)**

W art. 115 projektu zaproponowano jedną zmianę przepisów ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności<sup>21</sup>. Generalny Inspektor zgłaszał

---

<sup>21</sup> Dz. U. z 2016 r. poz. 217, 1579, 1948, dalej zwana ustawą o programach polityki spójności.

uwagi w procesie legislacyjnym dot. w/w aktu<sup>22</sup> oraz w toku jego nowelizacji w 2016 r.<sup>23</sup> **Większość z nich pozostaje aktualna.**

Odnosząc się do kwestii wskazania administratora danych, Generalny Inspektor, w obliczu sygnałów płynących od podmiotów uczestniczących w projektach europejskich, sugeruje zweryfikowanie, czy w przypadku procesów, w które zaangażowanych jest tak wiele podmiotów w różnych rolach, takie sztywne określenie jest zasadne. Ma to szczególne znaczenie, jeżeli może dochodzić do występowania współadministratorów danych.

**82. Zmiana ustawy z dnia 29 sierpnia 2014 r. o charakterystyce energetycznej budynków (Dz. U. z 2014 r. poz. 1200, z 2015 r. poz. 151 oraz z 2016 r. poz. 1250 i 1948)**

W art. 116 projektu sugeruje się pominięcie nowego ust. 5 jako zbędnego w związku treścią art. 31 ust. 1, w którym wskazano, kto odpowiada za prowadzenie wykazów. Użycie tego określenia powinno mieć miejsce, gdy w proces przetwarzania zaangażowana jest większa liczba podmiotów, ich rolę mogą się krzyżować albo nie będzie dochodzić do współadministrowania danymi osobowymi.

**83. Zmiana ustawy z dnia 28 listopada 2014 r. - Prawo o aktach stanu cywilnego (Dz. U. z 2016r. poz. 2064)**

W odniesieniu do zmiany 3 w art. 117 – wprowadzenie art. 5a do ustawy Prawo o aktach stanu cywilnego – wskazać należy, że nie jest wiadomo o jakie dokładnie dane chodzi w ust. 2 i ust. 3 przedmiotowego artykułu. Kwestia ta wymaga doprecyzowania.

**84. Zmiana ustawy z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (Dz. U. z 2017 r. poz. 1148)**

**W art. 118 projektu** sugeruje się pominięcie nowego ust. 3 jako zbędnego w związku treścią art. 21 oraz art. 22 ust. 1, w których wskazano, kto odpowiada za przygotowanie sprawozdań. Użycie określenia „administrator danych” powinno mieć miejsce, gdy w proces przetwarzania zaangażowana jest większa liczba podmiotów, ich rolę mogą się krzyżować albo nie będzie dochodzić do współadministrowania danymi osobowymi. Analogiczną uwagę

---

<sup>22</sup> DOLiS-033-220/14/KP/49867/ z dnia 1 lipca,

<http://orka.sejm.gov.pl/Druki7ka.nsf/0/7986AA47DBACB00DC1257D0B00363180/%24File/2450-003.pdf>

<sup>23</sup> DOLiS-033-592/16/KK/107359/ z dnia 13 grudnia,

<http://legislacja.rcl.gov.pl/docs//2/12292559/12394336/12394339/dokument264283.pdf>

należy zgłosić do treści art. 51 ust. 3 – projektodawca powinien wyjaśnić, czy nie dojdzie tutaj do stworzenia współadministratorów, na co wskazuje treść uzasadnienia do zmiany.

#### **85. Zmiana ustawy z dnia 24 lipca 2015 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw (Dz. U. poz. 1273, z późn. zm.)**

Odnosząc się do art. 121 projektowanej ustawy – przewidującego zmiany, GODO zauważa, iż biorąc pod uwagę zasadę minimalizacji danych konieczne jest stworzenie zamkniętego katalogu danych, poprzez usunięcie sformułowania „w szczególności” (art. 100f ust. 4)

Wątpliwości Generalnego Inspektora wzbudzają zaproponowane przez projektodawcę szerokie wyłączenia od stosowania przepisów RODO, polegające na zwolnieniu administratora z obowiązku informacyjnego, o którym mowa w art. 14 RODO, odstąpieniu od stosowania art. 15 oraz art. 18-21 RODO w zakresie, w jakim dane są niezbędne do zapewnienie realizacji zadań z art. 100f ustawy. Projektodawca zaproponował ponadto, aby art. 34 RODO nie był stosowany, jeśli administrator danych i informacji zgromadzonych w ewidencji przetwarzający dane osobowe na potrzeby ewidencji, w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej

Powyższe propozycje wyłączeń wymagają ponownej weryfikacji i ewentualnego dalszego doprecyzowania, w świetle argumentów przedstawionych powyżej odnośnie do art. 2 oraz art. 21 przepisów wprowadzających.

Zastrzeżenia GODO budzą również kwestie terminologiczne, przepisom RODO nie jest bowiem znane określenie „administrator danych i informacji”.

#### **86. Zmiana ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2017 r. poz. 1170)**

Nie mogą zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych, proponowane w – zmienionym przez art. 122 pkt 4 projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**) – art. 41 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej unormowania odnoszące się do przetwarzanie danych osobowych w sposób zautomatyzowany, w tym profilowania, przez zakłady ubezpieczeń.

Nie sposób pominąć, iż tak istotnym z punktu widzenia ochrony danych osobowych zagadnieniom został poświęcony zaledwie jeden artykuł, a postulowana regulacja sprowadza się w istocie do stwierdzenia: 1) zakłady ubezpieczeń mogą przetwarzać dane osobowe w sposób zautomatyzowany, w tym profilować, ubezpieczonych i ubezpieczających w celu wykonania obowiązku dokonania oceny ryzyka ubezpieczeniowego (art. 41 ust. 1b ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, który ma być dodany art. 122 pkt 4 lit. b projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**), 2) w celu wykonania obowiązku dokonania oceny ryzyka ubezpieczeniowego zakłady ubezpieczeń mogą przetwarzać dane osobowe dotyczące zdrowia ubezpieczonych lub uprawnionych z umowy ubezpieczenia (art. 41 ust. 1a ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, który ma być dodany art. 122 pkt 4 lit. b projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**), 3) przetwarzając dane osobowe ubezpieczonych lub uprawnionych z umowy ubezpieczenia oraz ubezpieczających zakłady ubezpieczeń są zwolnione z obowiązku, o którym mowa w art. 14 ust. 1 i 2 rozporządzenia unijnego (art. 41 ust. 2 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, w brzmieniu nadanym przez 122 pkt 4 lit. c projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**).

Już na wstępie zauważyć należy, że art. 41 ust. 1a ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (który ma być dodany art. 122 pkt 4 lit. b projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**) w zaproponowanym brzmieniu pozostaje w oczywistej sprzeczności z art. 22 ust. 4 rozporządzenia unijnego, co do zasady zakazującym podejmowania decyzji na podstawie zautomatyzowanego przetwarzania danych osobowych, w tym profilowania, opierającego się na szczególnych kategoriach danych osobowych, a więc również danych o stanie zdrowia (art. 22 ust. 4 w zw. z art. 9 ust. 1 rozporządzenia unijnego). Zgodnie z art. 22 ust. 4 rozporządzenia unijnego wyjątek od tego zakazu może być wprowadzony w prawie państwa członkowskiego ze względu na ważny interes publiczny, jednakże wymaga to, by w prawie tego państwa członkowskiego istniały właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Tymczasem w projektowanym art. 41 ust. 1a ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej brak jest jakichkolwiek unormowań w tym przedmiocie.

Nie do zaakceptowania przez organ do spraw ochrony danych osobowych jest także szczątkowość pozostałych regulacji z art. 41 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i

reasekuracyjnej odnoszących się do przetwarzania danych osobowych w sposób zautomatyzowany, w tym profilowania, przez zakłady ubezpieczeń.

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi zaprezentowane w art. 41 ust. 2 ustawy wyłączenie art. 14 ust. 1 i 2 rozporządzenia unijnego.

Jeśli chodzi o art. 41 ust. 3 ustawy o działalności ubezpieczeniowej i reasekuracyjnej, to stwierdzić należy, iż przepis ten wymaga ponownego zweryfikowania przez projektodawcę co do jego merytorycznej prawidłowości i zgodności z rozporządzeniem unijnym.

Oprócz powyższego – w związku z zaproponowaną zmianą do art. 38 ust. 6 ustawy o działalności ubezpieczeniowej i reasekuracyjnej organ do spraw ochrony danych osobowych przypomina, że istnieje w polskim porządku prawnym niespójność między art. 38 ust.1–7 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej a art. 26 ust. 3 pkt 7 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. O ile bowiem ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej upoważnia zakład ubezpieczeń do uzyskania (po spełnieniu warunków określonych w art. 38) informacji o stanie zdrowia ubezpieczonego lub osoby, na rachunek której ma zostać zawarta umowa ubezpieczenia, to art. 26 ust. 3 pkt 7 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta uprawnia podmiot udzielający świadczeń zdrowotnych do udostępnienia zakładowi ubezpieczeń, za zgodą pacjenta, dokumentacji medycznej. Prawo do informacji o stanie zdrowia i prawo do uzyskania dokumentacji medycznej nie są zaś tożsame.

#### **87. Zmiana ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowaniu dzieci (Dz. U. z 2016 r. poz. 195, z późn. zm.)**

W art. 126 projektu użyto sformułowań wskazujących na uprawnienie ministra właściwego do rodziny do przetwarzania danych osobowych (art. 14 ust. 3). Natomiast zgodnie z art. 6 ust. 1 lit. c RODO podstawą do przetwarzania może być jedynie obowiązek prawny ciążyący na administratorze. Obecne konstrukcja realizacji uprawnienia albo obowiązku wyrażona w art. 23 ust. 1 lit. b ustawy o ochronie danych osobowych nie będzie po 25 maja przyszłego roku dopuszczalna. Dlatego też konieczna jest zmiana brzmienia przepisu.

W projektowanym przepisie sformułowano również obowiązek przekazywania przez organy właściwe i marszałków województw danych do rejestru centralnego, z wykorzystaniem



systemów teleinformatycznych. Nie zostały jednak uregulowane tryb, zasady oraz częstotliwość przekazywania tych danych, sugeruje się zatem doprecyzowanie tych kwestii.

**88. Zmiana ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań z zakresu informatyzacji działalności organów Krajowej Administracji Skarbowej (Dz. U. z 2016 r. poz.781, 1948 i 2260)**

**W art. 128 projektu** – zmiana art. 17 ust. 1 – dokonuje się wyłączenia stosowania art. 12-22 i art. 34 RODO. Projektodawca powinien zweryfikować, czy takie całkowite ograniczenie wszystkich praw jest dopuszczalne z punktu widzenia przesłanek wskazanych w art. 23 RODO oraz czy wymogi określone w art. 23 ust. 2 RODO zostały spełnione. Uwagi poczynione powyżej w szczególności do art. 2 i 21 mają zastosowanie.

Należy podkreślić, że już obecnie obowiązujące przepisy ustawy o szczegółowych zasadach wykonywania niektórych zadań w zakresie informatyzacji działalności organów Krajowej Administracji Skarbowej naruszają zasadę celowości przetwarzania danych (art. 5 ust. 1 pkt b RODO). Dotyczy to art. 16 ww. ustawy, który zezwala spółce na pozyskiwanie i przetwarzanie danych obywateli zgromadzonych w rejestrach Krajowej Administracji Skarbowej oraz z innych zbiorów danych prowadzonych przez organy władzy publicznej.

Zgodnie z założeniami ww. ustawy (art. 1 i 2) celem powołanej spółki ma być zapewnienie organom KAS systemów teleinformatycznych wspierających działania mające na celu wykrywanie naruszeń prawa podatkowego. W ramach ww. zadań spółka ma wykonywać zadania w zakresie a) budowy systemów teleinformatycznych, oraz b) rozbudowy lub unowocześniania istniejących systemów teleinformatycznych. W ustawie **nie wskazuje się, że celem działalności spółki ma być przetwarzanie danych** na zlecenie ministra właściwego do spraw finansów publicznych oraz Krajowej Administracji Skarbowej. Tymczasem na mocy art. 16 ww. ustawy powołanej spółce celowej daje się możliwości dostępu do danych przetwarzanych w systemach teleinformatycznych ministra właściwego ds. finansów oraz do danych przetwarzanych w rejestrach innych organów władzy publicznej. Jak wskazano w opinii GIODO z 18 lutego 2016 r. dostęp do ww. danych nie jest niezbędny do realizacji celu określonego w art. 2 ust. 2, tj. do budowy lub rozbudowy systemów informatycznych mających służyć organom KAS do wykrywania naruszania przepisów prawa podatkowego, w oparciu o dane uzyskiwane z systemów teleinformatycznych ministra właściwego do spraw finansów publicznych oraz Krajowej Administracji Skarbowej. W celu opracowania ww. narzędzi informatycznych wystarczające jest uzyskanie dostępu do struktury danych, które będą przetwarzane/poddawane analizie przy wykorzystaniu ww. narzędzi, nie zaś do treści zapisanych

danych. W nawiązaniu do powyższego należy zauważyć, że dobre praktyki dotyczące budowy oprogramowania zakazują co do zasady wykorzystywania danych rzeczywistych przez zespoły developerski do przeprowadzania testów z uwagi na ochronę danych. Użycie danych rzeczywistych dopuszczalne jest jedynie w odniesieniu do testów integracyjnych, które przeprowadzane są na ogół we współpracy z administratorem danych i pod jego nadzorem.

Wprowadzone zmiany w art. 17 ust. 1 zmiany wyłączające powołaną spółkę z obowiązków stosowania art. 12 - 22 i art. 34 RODO narusza art. 51 ust 4 Konstytucji RP, który stanowi, że *„Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą”* oraz zasadę RODO dotyczącą prawidłowości danych zawartą w art. 5 ust. 1 litera d) RODO. Wprowadzone zmiany wyłączający powołaną spółkę z obowiązków stosowania art. 16 RODO wprost narusza ww. prawa osób zagwarantowane art. 51 ust 4 Konstytucji RP i zasadę zawartą w art. 5 ust. 1 litera d) RODO. Wprowadzone zmiany w art. 17 ust. 1 zmiany wyłączające powołaną spółkę z obowiązków stosowania art. 12 - 22 i art. 34 RODO narusza również art. 61 ust 1 Konstytucji RP stanowiący, że *„Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.”* Wprowadzone ograniczenia stosowania RODO odnoszą się nie tylko do informowania osób o tym, że ich dane są w określony sposób przetwarzane, co w niektórych okolicznościach może być uzasadnione, ale również do braku ogólnych informacji o sposobie przetwarzania danych przez spółkę, w tym informacji o zautomatyzowanym podejmowaniu decyzji i istotnych informacji dotyczących zasad ich podejmowania (art. 14 ust 2 pkt g RODO). Brak informacji o sposobie przetwarzania przez spółkę danych pozyskanych z różnych rejestrów państwowych, w tym sprawowanie nadzoru nad tym przetwarzaniem nie przez ministra właściwego do spraw finansów publicznych oraz Krajowej Administracji Skarbowej lecz przez powołanego przez spółkę pełnomocnika nie daje gwarancji właściwego nadzoru nad przetwarzanymi przez spółkę danymi przez ich administratora.

Projektodawca powinien zweryfikować, czy nie jest koniecznym wprowadzenie innych zmian w przepisach ustawy, na które w toku prac legislacyjnych<sup>24</sup> oraz nowelizacji przepisów ustawy zwracał uwagę Generalny Inspektor Ochrony Danych Osobowych.

---

<sup>24</sup> DOLiS-033-39/16/KK/10751/ z dnia 18 lutego 2016 r.,  
<http://legislacja.rcl.gov.pl/docs/2/12281951/12336135/12336138/dokument212284.pdf>

**89. Zmiana ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym (Dz. U. poz. 862 i 1948)**

W zakresie art. 129 projektu – zmienianym art. 5 ust. 2 – zbędnym wydaje się dookreślenie, iż minister jest administratorem danych. Użycie tego określenia powinno mieć miejsce, gdy w proces przetwarzania zaangażowana jest większa liczba podmiotów, ich rolę mogą się krzyżować albo nie będzie dochodzić do współadministrowania danymi osobowymi, o którym mowa w art. 26 RODO.

Projektodawca powinien wyjaśnić intencję, która przyświecała ograniczeniu praw osób, których dane dotyczą w nowym **art. 17 ust. 3a**, w sytuacji gdy w art. 17 ust. 1 mowa jest o wykorzystywaniu danych z rejestru bez danych osobowych (wyłączenie danych wskazanych w art. 7 ust. 3 pkt 1 i 2) oraz zanonimizowaniu dla celów statystycznych. Wydaje się, że będzie to regulacja pusta.

**90. Zmiana ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. poz. 1947, z późn.zm.)**

Generalny Inspektor Ochrony Danych Osobowych zwraca uwagę na propozycję ograniczenia zastosowania art. 12 – 22, art. 34 RODO w art. 35 ust.5 art. 45 ust. 1a, art. 47, art. 127 ust. 1a. Wprowadzanie ograniczeń w zakresie art. 12-22 RODO i art. 34 RODO, z pominięciem wskazania elementów określonych w art. 23 ust. 2 RODO, oznacza niedopuszczalność wyłączenia ww. przepisów RODO (patrz uwaga do art. 2 i art. 21 przepisów wprowadzających).

Realizacja obowiązku informacyjnego i prawa do kontroli procesu przetwarzania danych osobowych nie powinny być całkowicie ograniczone, gdyż narusza to autonomię informacyjną osoby określoną w art. 51 Konstytucji. Nie należy dopuszczać do sytuacji, w której po zebraniu informacji i zakończeniu niezbędnych czynności osoba nie będzie poinformowana o tym fakcie. Jest to niezbędne, aby możliwe była realizacja prawa ujętego w art. 51 ust. 3 Konstytucji.

Zastrzeżenia GIODO budzi nieskonkretyzowany katalog danych osobowych wskazany w art. 45 ust. 1 oraz art. 47 ust. 1, który powinien być wyraźnie i wyczerpująco określony w przepisach rangi ustawowej. Tak szerokie uprawnienie należy uznać dodatkowo za nieproporcjonalne i z art. 51 ust. 2 i 5 Konstytucji, zgodnie z którymi władze publicznie nie mogą przetwarzać informacji o obywatelach innych niż niezbędne w demokratycznym państwie prawnym, a zasady i tryb przetwarzania określa ustawa.

Wątpliwości GIODO budzi proponowany art. 147 ust. 2, w którym wyrażenie „mogą być zbierane” należy zastąpić sformułowaniem „są zbierane”.

**91. Zmiana ustawy z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz.U. poz. 2072)**

Należy wskazać, że uwagi do art. 131 analogiczne jak uwagi do art. 106 projektu.

**92. Zmiana ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2017 r. poz. 59 i 949).**

Należy zauważyć, iż zaproponowana nowelizacja dotyczy wyłącznie szkół artystycznych i placówek prowadzonych lub nadzorowanych przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego. Taka regulacja wydaje się niepełna, zatem Generalny Inspektor wskazuje na potrzebę dokonania przez projektodawcę dodatkowej analizy w tym zakresie. Niezależnie od powyższego, zastrzeżenia organu wzbudzają następujące kwestie.

Biorąc pod uwagę zasadę minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c RODO sugeruje się stworzenie zamkniętych katalogów danych, poprzez usunięcie sformułowania „w szczególności” (*vide* proponowane brzmienie art. 188a ust. 1).

Nie jest zrozumiałe generalnie uprawnienie do przetwarzania takich danych jak: wykształcenie, miejsce pracy i zajmowane stanowisko, w tym wysokość wynagrodzenia oraz numer rachunku bankowego. Niewątpliwie w indywidualnych przypadkach pozyskiwanie takich danych może być uzasadnione, jednak przepisy powinny takie okoliczności wskazywać, zamiast tworzyć ogólny przepis pozwalający na przetwarzanie tak szczegółowych informacji.

Jednocześnie w przypadku przetwarzania danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych – mając na uwadze, że w polskim porządku prawnym nie istnieje obowiązek posiadania przez osoby fizyczne takich środków komunikacji – należy pozostawić swobodę możliwości podawania takich danych.

Wątpliwości Generalnego Inspektora wzbudzają zaproponowane przez projektodawcę szerokie wyłączenia od stosowania przepisów RODO, polegające na odstąpieniu od stosowania art. 13, art. 14 oraz art. 17-19 RODO w zakresie, w jakim dane są niezbędne do zapewnienie realizacji zadań, o których mowa w ustawie oraz odstąpieniu od stosowania art. 5 ust. 2 RODO – w zakresie obowiązków wykazywania przestrzegania przepisów art. 5 ust. 1 rozporządzenia. Wyłączone zostało ponadto stosowanie art. 34 RODO – w przypadku, gdy administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej Biuletynu Informacji publicznej lub na swojej stronie internetowej. Ograniczone zostało również stosowanie art. 12 oraz art. 15 RODO. Zagadnienia te wymagają

ponownej weryfikacji i ewentualnego dalszego doprecyzowania, w świetle argumentów przedstawionych powyżej odnośnie do art. 2, art. 21 oraz art. 28 przepisów wprowadzających.

Odnosząc się do projektowanego art. 188a ust. 6 ustawy – Prawo oświatowe, GODO zauważa, iż okres retencji danych sformułowany został w sposób nieprecyzyjny, stanowi bowiem w istocie powtórzenie zasady ogólnej, sugeruje się zatem jego dookreślenie. Art. 188a ust. 8 zakłada możliwość zlecenia przetwarzania danych osobowych lub pełnienie funkcji podmiotu przetwarzającego te dane osobowe na zlecenie innego podmiotu przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego, specjalistyczną jednostkę nadzoru, dyrektora szkoły artystycznej lub placówki prowadzonej lub nadzorowanej przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego. Z uwagi na zbyt ogółe i nieostre sformułowanie tej propozycji przepisu, powtórzenia wymagają uwagi wyrażone powyżej w odniesieniu do art. 21 projektu.

### **93. Zmiana ustawy z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami (Dz. U. poz. 648)**

**W art. 133 projektu** Generalny Inspektor proponuje rozważyć nową regulację art. 10 zmienianej ustawy – wyczerpującego wskazania zakresu danych niezbędnych do identyfikacji podmiotu. Uwagę w tym zakresie zgłoszono w toku uzgodnień projektu ustawy w 2016 r.<sup>25</sup>

Zastrzeżenia GODO budzą również przepisy zawarte w **rozdziale 3 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych** – Przepisy uchylające, dostosowujące i przejściowe

W świetle – mającej swoje oparcie w art. 2 Konstytucji Rzeczypospolitej Polskiej – zasady prawidłowej legislacji za zasadniczy brak rozdziału 3 projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych** uznać należy nieuregulowanie w przepisach uchylających, dostosowujących i przejściowych kwestii kontynuowania kadencji Generalnego Inspektora Ochrony Danych Osobowych po dniu 24 maja 2018 r., czyli po dacie rozpoczęcia stosowania w polskim porządku prawnym rozporządzenia unijnego. Podkreślenia wymaga, iż jedynie w uzasadnieniu projektu na str. 12, 28, 51, 105 i 109 znalazło się następujące sformułowanie: „Generalny Inspektor Ochrony Danych Osobowych w wyniku zmian wprowadzonych ustawą o ochronie danych osobowych stanie się Prezesem Urzędu Ochrony Danych Osobowych”.

---

<sup>25</sup> DOLiS-033-193/16/KK/52858/ z dnia 13 czerwca 2016 r.,  
<http://legislacja.rcl.gov.pl/docs//2/12285652/12354079/12354082/dokument253485.pdf>

Przypomnieć należy, iż aktualny piastun organu administracji publicznej do spraw ochrony danych osobowych, którym – zgodnie z art. 8 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych – jest Generalny Inspektor Ochrony Danych Osobowych, sprawuje swoją funkcję od dnia 9 kwietnia 2015 r., zaś – w myśl art. 8 ust. 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych – jego kadencja biegnie od dnia 22 kwietnia 2015 r. i winna zakończyć się w dniu 22 kwietnia 2019 r. Tymczasem – stosownie do dyspozycji art. 20 ust. 1 projektowanej ustawy o ochronie danych osobowych, która to ustawa ma wejść z dniem 25 maja 2018 r. (art. 1 projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych**) – organem właściwym w sprawie ochrony danych osobowych jest (od dnia 25 maja 2018 r.) Prezes Urzędu Ochrony Danych Osobowych. Wobec pominięcia tego zagadnienia w przepisach uchylających, dostosowujących i przejściowych projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych** powstaje więc pytanie o wpływ utworzenia organu właściwego w sprawie ochrony danych osobowych – Prezesa Urzędu Ochrony Danych Osobowych na trwającą w dniu 25 maja 2018 r. kadencję Generalnego Inspektora Ochrony Danych Osobowych.

Nie można przy tym pominąć, że w świetle art. 54 ust. 1 lit. d rozporządzenia unijnego kadencja organu nadzorczego trwa minimum cztery lata, zaś dopuszczalne jest jedynie częściowe skrócenie pierwszej kadencji po dniu 24 maja 2016 r. i tylko wtedy, jeżeli jest to niezbędne, aby chronić niezależność organu nadzorczego w drodze procedury stopniowej wymiany członków.

Również w wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. w sprawie C-288/12 Komisja Europejska vs Węgry stwierdzono, iż skrócenie – przez Węgry – kadencji organu nadzorczego ochrony danych osobowych stanowiło uchybienie zobowiązaniom, które ciążyą na tym państwie członkowskim na mocy *dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (Dz. Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.).

Tym samym w przepisach uchylających, dostosowujących i przejściowych projektu **ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych** winny znaleźć się regulacje przewidujące objęcie w dniu 25 maja 2018 r. przez aktualnego Generalnego Inspektora Ochrony Danych Osobowych funkcji Prezesa Urzędu Ochrony Danych Osobowych przynajmniej na okres do dnia 22 kwietnia 2019 r.

Jeśli jednak – wbrew literalnemu brzmieniu art. 54 ust. 1 lit. d rozporządzenia unijnego, który to przepis dopuszcza częściowe skrócenie pierwszej kadencji po dniu 24 maja 2016 r. (a kadencja aktualnego Generalnego Inspektora Ochrony Danych Osobowych trwa od dnia 22 kwietnia 2015 r.), oraz wbrew wyrokowi Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. w sprawie C-288/12 Komisja Europejska vs Węgry – zamiarem Projektodawcy było skrócenie kadencji Generalnego Inspektora Ochrony Danych Osobowych, jest on zobowiązany zamieścić w rozdziale 3 projektu **ustawy –Przepisy wprowadzające ustawę o ochronie danych osobowych** unormowanie formalnie znoszące organ do spraw ochrony danych osobowych –Generalnego Inspektora Ochrony Danych Osobowych, by przepis ten mógł zostać poddany procedurze notyfikacji zgodnie z art. 51 ust. 4 rozporządzenia unijnego.

**94. W odniesieniu do art. 136 projektu** należy zauważyć, iż Generalny Inspektor Ochrony Danych Osobowych nie włada mieniem Skarbu Państwa. Mienie Skarbu Państwa służące do wykonywania zadań Generalnego Inspektora znajduje się we władaniu Biura Generalnego Inspektora Ochrony Danych Osobowych, przy pomocy którego GODO wykonuje swoje zadania. Ponadto należy wskazać, iż w treści projektowanego przepisu zastosowano formułę (skrót) mogącą wskazywać, iż Prezes Urzędu Ochrony Danych Osobowych może, niezależnie od Skarbu Państwa, być właścicielem mienia.

**95. Podobną uwagę należy zgłosić do treści art. 137 projektu.** Należności i zobowiązania związane z funkcjonowaniem Generalnego Inspektora Ochrony Danych Osobowych stanowią należności i zobowiązania Skarbu Państwa reprezentowanego przez Biuro Generalnego Inspektora Ochrony Danych Osobowych jako państwową jednostkę organizacyjną.

**96. W art. 138** błędnie odwołano się w treści przepisu do art. 147, zamiast do art. 146.

**97. Poważne wątpliwości art. 147 projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych,** gdyż w swojej aktualnej postaci skutkowałby automatyczną utratą mocy obowiązującej całej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych po upływie 30 dni od dnia zamieszczenia w Dzienniku Ustaw uchwalonej przez Parlament i podpisanej przez Prezydenta Rzeczypospolitej Polskiej *ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych,* a więc niekoniecznie w dniu 25 maja 2018 r., gdy w polskim porządku prawnym zaczną być stosowane rozporządzenie unijne.

## **98. Konieczność nowelizacji innych ustaw, które nie znalazły się w projekcie ustawy- Przepisy wprowadzające ustawę o ochronie danych**

Jednocześnie Generalny Inspektor zauważa – czemu dawał wyraz m.in. w swoich dotychczasowych wystąpieniach, jak i opiniach do projektów legislacyjnych – iż wiele jest zagadnień i przepisów wymagających przeglądu i analizy ich zgodności z postanowieniami RODO, a które nie znalazły miejsca w niniejszym projekcie. Przykładowo wskazać tu można przepisy ustawy – Prawo zamówień publicznych, ustawy o opiniodawczych zespołach sądowych specjalistów, ustawy o usługach płatniczych, przepisy dot. zarządzania kryzysowego. W tym zakresie GODO będzie sukcesywnie przedstawiał swoje dalsze stanowisko. Poniżej Generalny Inspektor wskazuje inne przykładowe zagadnienia wymagające dodatkowej analizy.

Ponadto, jak już zostało zauważone wyżej, do tej pory nie są znane Generalnemu Inspektorowi informacje na temat stanu prac legislacyjnych mających na celu implementację przepisów Dyrektywy 2016/680 do polskiego porządku prawnego.

### **Ustawa o promocji zatrudnienia i instytucjach rynku pracy**

W opinii Generalnego Inspektora Ochrony Danych Osobowych dostosowania do RODO wymagają przepisy ustawy z dnia 20 kwietnia 2004 roku o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2017 r. poz. 1065, z późn. zm.), zwłaszcza w zakresie, w jakim dotyczą one kwestii profilowania pomocy dla bezrobotnych. Aktualne pozostają zastrzeżenia, jakie Generalny Inspektor zgłaszał zarówno podczas prac legislacyjnych dotyczących rządowego projektu ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw, uchwalonego następnie przez Parlament i podpisanego przez Prezydenta Rzeczypospolitej Polskiej jako ustawa z dnia 14 marca 2014 roku o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw (Dz. U. z 2014 r. poz. 598), jak i przypomniane m. in. w piśmie z dnia 22 grudnia 2015 r. (znak: DOLiS-072-37/15/BG/107395/15), skierowanym do Minister Rodziny, Pracy i Polityki Społecznej.

Zastrzeżenia organu wzbudził fakt, iż na poziomie przepisów wykonawczych uregulowano tak zasadnicze kwestie, jak problematykę katalogu danych, w oparciu o które budowany jest profil bezrobotnego (§2), sposób ustalania profilu bezrobotnego (§3 i 4) oraz jego zmiany (§9). Równocześnie całkowitym milczeniem (zarówno w ustawie o promocji zatrudnienia i instytucjach



rynku pracy, jak i rozporządzeniu Ministra Pracy i Polityki Społecznej w sprawie profilowania pomocy dla bezrobotnego) pominięto m.in. zagadnienie okresu przechowywania danych bezrobotnego pozyskanych na potrzeby profilowania oraz samego wyniku operacji, która na tych danych została przeprowadzona, czy też możliwości żądania przez bezrobotnego usunięcia (zmiany) przyznanego mu profilu oraz dostępu do danych zebranych na jego temat. Kolejnym problemem, na który zwrócić trzeba uwagę przy ocenie obowiązujących rozwiązań dotyczących profilowania bezrobotnych, jest pozorne oparcie się przez ustawodawcę na zgodzie na profilowanie. Nie może bowiem umknąć uwadze art. 33 ust. 4 pkt 1 a ustawy o promocji zatrudnienia i instytucjach rynku pracy, zgodnie z którym osobę niewyrażającą zgody na ustalenie dla niej profilu (co wiąże się przecież z dokonaniem analizy jej danych przez powiatowy urząd pracy) pozbawia się statusu bezrobotnego i uprawnień związanych z tym statusem.

Rozwiązania powyższe są nie do pogodzenia z art. 22 RODO. Podleganie decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec osoby, której dane dotyczą skutki prawne lub w podobny sposób istotnie na nią wpływa jest bowiem – zgodnie z art. 22 ust. 2 lit. b – możliwe wówczas, gdy taka decyzja jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Decyzje te nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Inne istotne zagadnienia, pozostające we właściwości Ministra Rodziny, Pracy i Polityki Społecznej, na które należy zwrócić uwagę w kontekście RODO to:

- konieczność kompleksowego uregulowania w przepisach prawa zasad i sposobu prowadzenia dokumentacji przez psychologów (*vide* – wystąpienie GIODO z dnia 23 marca 2017 r., skierowane do Minister Rodziny, Pracy i Polityki Społecznej znak: DOLiS-023-124/17/BG/24373/17),
- konieczność zmiany przepisów rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. z 1996 r. Nr 62, poz. 286, z późn.

zm.), *vide* – wystąpienie GIODO z dnia 22 grudnia 2016 r., skierowane do Minister Rodziny, Pracy i Polityki Społecznej znak: DOLiS-035-2141/16/BG/109854/16.

### **Ustawa o utrzymaniu czystości i porządku w gminach**

Generalny Inspektor Ochrony Danych Osobowych zgłasza również wątpliwości w zakresie regulacji związanych z koniecznością udostępniania danych osobowych w treści deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi zawartych **w ustawie z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach**. W opinii organu do spraw ochrony danych osobowych obecne przepisy zawarte w wyżej wskazanej ustawie mogą prowadzić do nadmiernej ingerencji w prywatność osób fizycznych.

Zgodnie z art. 6m ustawy o utrzymaniu czystości i porządku w gminach, właściciel nieruchomości jest obowiązany złożyć do wójta, burmistrza lub prezydenta miasta deklarację o wysokości opłaty za gospodarowanie odpadami komunalnymi w terminie 14 dni od dnia zamieszkania na danej nieruchomości pierwszego mieszkańca lub powstania na danej nieruchomości odpadów komunalnych (ust. 1). Deklaracja zawiera **dane niezbędne do określenia wysokości opłaty za gospodarowanie odpadami komunalnymi** oraz wysokość opłaty za gospodarowanie odpadami komunalnymi (ust. 1a).

Zgodnie z ust. 1b, rada gminy określając wzór deklaracji może wymagać podania następujących danych: 1) imię i nazwisko lub nazwę właściciela nieruchomości oraz adres miejsca zamieszkania lub siedziby; 2) adres nieruchomości; 3) dane stanowiące podstawę zwolnienia z opłaty za gospodarowanie odpadami komunalnymi; 4) numer telefonu właściciela nieruchomości; 5) adres poczty elektronicznej właściciela nieruchomości; 6) inne informacje niezbędne do wystawienia tytułu wykonawczego.

W opinii Generalnego Inspektora, wskazany powyżej zakres danych jest zbyt szeroki do realizacji celów wynikających z ustawy o utrzymaniu czystości i porządku w gminach.

Obecne rozwiązanie, tj. możliwość pozyskiwania za pośrednictwem deklaracji „innych informacji niezbędnych do wystawienia tytułu wykonawczego” stwarza ryzyko potencjalnych nadużyć. Przykładowo, niektóre gminy żądają od właścicieli nieruchomości udostępnienia w treści deklaracji informacji o miejscu zatrudnienia czy też **danych dotyczących kont bankowych (np. pełny numer rachunku bankowego właściciela nieruchomości)**. Zbieranie tak szerokiego zakresu danych od wszystkich mieszkańców jedynie w celu ułatwienia egzekucji należności od osób, które nie wywiązują się z obowiązku uiszczenia opłaty za gospodarowanie odpadami komunalnymi

stanowi nieproporcjonalną ingerencję w ich prywatność. Trudno przy tym uznać takie dane za „niezbędne do określenia wysokości opłaty za gospodarowanie odpadami komunalnymi”.

Obecne przepisy przewidują również, że rada gminy może wymagać od właściciela nieruchomości podania jego **numeru telefonu oraz adresu poczty elektronicznej**. W praktyce, przedłożenie tych danych może zatem stać się obowiązkiem, zamiast wyłącznie możliwością. Nie kwestionując fakultatywności podawania tego typu informacji w treści deklaracji, nie można jednocześnie wyrazić aprobaty wobec ich wymuszania poprzez wprowadzenie obowiązkowego pola w deklaracji. Powyższe pozostaje wątpliwe, albowiem w polskim porządku prawnym nie istnieje obowiązek posiadania telefonu czy poczty elektronicznej. Takiego obowiązku nie powinny nakładać komentowane przepisy – zatem wskazane wyżej dane powinny być traktowane jako fakultatywne.

Nie może dochodzić do sytuacji, w której to rada gminy, w sposób *de facto* dowolny, kształtować będzie zakres danych, jakie mogą być pozyskiwane od właścicieli nieruchomości. Konieczne jest zatem uspoźnienie systemu na poziomie centralnym, tak, aby w przepisach ustawy zawarty został precyzyjny, zamknięty katalog danych osobowych, jakie mogą być przetwarzane. Dane te muszą być przy tym adekwatne, innymi słowy rzeczywiście niezbędne do realizacji celów wynikających z przepisów ustawy o utrzymaniu czystości i porządku w gminach.

### **Zmiana ustawy o samorządzie gminnym**

Generalny Inspektor Ochrony Danych Osobowych zwraca uwagę, że w przedłożonym projekcie nie znalazły się propozycje dotyczące ustaw samorządowych, m.in. propozycja zmiany ustawy z dnia 8 marca 1990 r. o samorządzie gminnym.. W opinii GODO przepisy powyższej ustawy powinny zostać doprecyzowane we wskazanym poniżej zakresie.

W pierwszej kolejności Generalny Inspektor zwraca się z wnioskiem do Projektodawcy o rozważenie uregulowania w ustawie o samorządzie gminnym jasnych kryteriów przetwarzania danych osobowych gromadzonych podczas konsultacji społecznych w szczególności w zakresie głosowania na poszczególne projekty w ramach budżetu partycypacyjnego. Organ do spraw ochrony danych osobowych postulował już wniesienie zmian w tym zakresie kierując wystąpienie do Ministra spraw Wewnętrznych i Administracji (pismo z dnia 29 sierpnia 2017 r. sygn. DOLiS-027-863/17/AG/65742).

Kwestia konsultacji społecznych jest przedmiotem regulacji ustawy o samorządzie gminnym, gdzie **w art. 5 a ust. 2** wskazuje się, że zasady i tryb przeprowadzania konsultacji

z mieszkańcami gminy określa uchwała rady gminy. W opinii GIODO zasadnym jest jednak uregulowanie w przepisach rangi ustawy szczególnych w stosunku do ogólnych norm ustawy o ochronie danych osobowych, zasad przetwarzania danych osobowych na potrzeby przeprowadzania konsultacji społecznych w formie głosowania nad projektami budżetu partycypacyjnego.

Generalny Inspektor Ochrony Danych Osobowych zwraca również uwagę na regulację zawartą w **art. 10b ust. 2 i 3** ustawy o samorządzie gminnym, w myśl którego *rada gminy w odniesieniu do jednostek obsługiwanych, o których mowa w art. 10 a pkt 1, określa w drodze uchwały, w szczególności 1) jednostki obsługujące, 2) jednostki obsługiwane, 3) zakres obowiązków powierzonych jednostkom obsługującym w ramach wspólnej obsługi; Jednostki obsługiwane, o których mowa w art. 10 a pkt 2 i 3, mogą na podstawie porozumień zawartych przez te jednostki z jednostką obsługującą, przystąpić do wspólnej obsługi, po uprzednim zgłoszeniu tego zamiaru wójtowi. zakres wspólnej obsługi określa zawarte porozumienie.*

Także w tym przypadku w opinii organu do spraw ochrony danych osobowych zasadnym byłoby rozważenie uregulowania kwestii „wspólnej obsługi” w ustawie. Odsyłanie tak istotnych kwestii do uchwał, a zwłaszcza do porozumień, nie będących źródłem powszechnie obowiązującego prawa, nie może zyskać akceptacji Generalnego Inspektora. Obecna konstrukcja przepisu pozostawia zbyt duży zakres dowolności jednostkom uczestniczącym w procesie wspólnej obsługi poprzez uprawnienie ich do określania istotnych dla podejmowanych działań kwestii wedle wyboru – w formie uchwały albo porozumienia.

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi również konstrukcja art.10 d ustawy o samorządzie gminnym, który reguluje kwestię przetwarzania danych osobowych w ramach wspólnej obsługi administracyjnej, finansowej i organizacyjnej gmin. W opinii organu do spraw ochrony danych osobowych koniecznym jest doprecyzowanie w powyższym przepisie, jakie role mają pełnić jednostka obsługująca i jednostka obsługiwana. Przepisy powinny określać, czy dany podmiot pełni rolę administratora, czy też np. podmiotu, któremu zostało powierzone przetwarzanie danych etc. Brak określenia przez ustawodawcę ról powyższych podmiotów budzi wątpliwości w kwestii odpowiedzialności za przetwarzane dane. Dodatkowo art. 10 d stanowi o „przetwarzaniu danych osobowych jednostki obsługiwanej”. Takie brzmienie przepisu jest zbyt ogólne, nie precyzuje, że w istocie chodzi nie o „dane osobowe jednostki obsługiwanej” lecz dane osobowe osób fizycznych (podmiotów danych) przetwarzane przez jednostkę obsługującą w ramach wykonywania wspólnej obsługi.

