Uzasadnienie

do projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych

W dniu 25 maja 2016 r. weszło w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwane dalej „rozporządzeniem 2016/679". Rozporządzenie 2016/679 zacznie być aktem bezpośrednio stosowanym od dnia 25 maja 2018 r. i do tego czasu każde z państw członkowskich zobowiązane jest do zapewnienia jego skutecznego stosowania w swoim porządku prawnym poprzez przyjęcia właściwych przepisów wewnętrznych. Tym samym, począwszy od tej daty, polskie przepisy muszą zapewniać skuteczne stosowanie przepisów rozporządzenia 2016/679, nie powielając rozwiązań rozporządzenia ani nie będąc z nim sprzecznymi. W tym celu konieczne jest poza uchwaleniem nowej ustawy o ochronie danych osobowych także dokonanie licznych zmian w innych ustawach zapewniających dostosowanie krajowego porządku prawnego do nowych norm prawnych Z uwagi na ich liczbę zdecydowano się dokonać tego w projekcie ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych.

W projekcie ustawy zawarto szereg zmian ustaw, wypracowanych wspólnie z właściwymi resortami, zapewniających dostosowanie krajowego porządku prawnego do nowych norm prawnych zawartych w rozporządzeniu 2016/679. W kolejnych punktach omówione zostaną zmiany dokonywane w projekcie ustawy.

Projekt ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych zwiera poza przepisami zmieniającymi także przepis uchylający ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych a także przepisy dostosowujące oraz przejściowe.

W kolejnych punktach omówione zostaną zmiany wprowadzane w poszczególnych ustawach. W przypadku gdy zmiany w różnych ustawach pozostających tym samym obszarze działania dotyczyły tych samych kwestii, zmiany omówiono łącznie.

1. Ustawa z dnia 17 czerwca 1966 o postępowaniu egzekucyjnym w administracji

Zmiana w art.2 – dodanie § 1 pkt 12

Zmiana ma charakter dostosowawczy i związana jest ze zmianą organu właściwego w sprawach ochrony danych osobowych. Zmiana polega na zastąpieniu odwołania do Generalnego Inspektora Danych Osobowych odwołaniem do Prezesa Urzędu Ochrony Danych Osobowych.

Zmiana w art. 36 – dodanie § 4

Propozycja dodania § 4 do art. 36 dopuszcza, w sytuacji opisanej w § 1, możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i art. 34 RODO. Ograniczenie praw podmiotów danych jest możliwe na podstawie art. 23 ust. 1 lit. d i e RODO, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym 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 oraz 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. W przypadku art. 36 § 1 ograniczenie to zostało zastosowane w zakresie niezbędnym do realizacji zdań publicznych przez organy egzekucyjne i wierzycieli.

Przepis został uzupełniony ponadto o 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.

2. Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych, ustawa z dnia 9 października 2009 r. o dyscyplinie wojskowej, ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawie z dnia 29 maja 1974 r. o zaopatrzeniu inwalidów wojennych i wojskowych oraz ich rodzin.

Obowiązek obrony Rzeczypospolitej Polskiej wynika z art. 85 Konstytucji RP. Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej określa zakres praw i obowiązków obywateli i organów związanych z realizacją powszechnego obowiązku obrony Rzeczypospolitej Polskiej, w tym zbieranie, zakres, przetwarzanie, udostępnianie i przechowywania danych osobowych.

W związku z powyższym w ww. ustawach proponuje się wyłączenie praw określonych w szczególności w następujących przepisach rozporządzenia 2016/679:

1) art. 14 – ewidencja wojskowa jest w dużej mierze uzupełniana danymi, które pozyskiwane są od innych pomiotów, niż osoba, której dane dotyczą. Na podstawie przepisów art. 49 ust. 2b ustawy o powszechnym obowiązku obrony RP jest aktualizowana (w cyklu miesięcznym) danymi pozyskiwanym z rejestrów państwowych. Ponadto, zgodnie z przepisami art. 50 i 51, wojskowi komendanci uzupełnień pozyskują niektóre dane dotyczące osoby, następnie gromadzone i przetwarzane w ewidencji wojskowej, nie od osoby której te dane dotyczą lecz od innych podmiotów, tj.:

a) pracodawców (w zakresie zatrudnienia, zwolnienia oraz kwalifikacjach i zajmowanym stanowisku),
b) rektorów szkół wyższych, dyrektorów zakładów kształcenia nauczycieli, dyrektorów szkół ponadgimnazjalnych (w zakresie przyjęcia do szkoły, czasu trwania nauki, powtarzaniu roku/semestru, skreślenia z listy uczniów/studentów, wydaleniu ze szkoły, uzyskaniu statusu absolwenta /ukończenia nauki),
c) sądów (w zakresie zastosowania tymczasowego aresztowania, prawomocnego skazania),
d) zakładów karnych, poprawczych i aresztów śledczych (w zakresie informacji o osadzeniu w tych zakładach/aresztach lub zwolnieniu z nich).

Zakres pozyskiwanych w ten sposób danych jest na tyle szeroki, że nie widzi się możliwości informowania osobę przez administratora w zakresie, o którym mowa w art. 14 rozporządzenia 2016/679;

2) art. 17 i art. 21 – dane osobowe w ewidencji wojskowej są gromadzone i przetwarzane w celu realizacji zadań z zakresu powszechnego obowiązku obrony. Żądanie usunięcia tych danych przez osobę, której dotyczą lub zgłoszenie sprzeciwu wobec przetwarzania dotyczących

jej danych uniemożliwiłoby właściwe administrowanie rezerwami osobowymi dla celów powszechnego obowiązku obrony;

3) art. 19 – w art. 49 ust. 1d ustawy o powszechnym obowiązku obrony RP ustawodawca szczegółowo określa podmioty, którym mogą być udostępniane dane o osobie zgromadzone w ewidencji wojskowej. Szeroki katalog tych podmiotów uniemożliwia informowanie o każdym przypadku sprostowania, usunięcia lub ograniczenia przetwarzania danych. Ponadto liczba osób, których dane zgromadzone są w ewidencji wojskowej (szacunkowo około 8 mln) wyklucza, aby administrator informował wszystkie te osoby, których dane dotyczą o odbiorcach tych danych;

4) art. 20 – wojskowy komendant uzupełnień (administrator) prowadzi ewidencję wojskową (tj. gromadzi i przetwarza dane o osobach) na terenie objętym zakresem jego działania (opartym o miejsce stałego lub czasowego pobytu osób). Szczegółowe rozwiązania w tym zakresie określają przepisy rozporządzenia Ministra Obrony Narodowej z dnia 8 października 2010 r. w sprawie prowadzenia ewidencji wojskowej (Dz. U. Nr 199, poz. 1321, z późn. zm.). Podkreślenia ponadto wymaga, że w ewidencji wojskowej mogą być również gromadzone dane, które stanowią informacje niejawne. Dlatego też nie widzi się możliwości, aby żądanie osoby, której dane dotyczą decydowało o przekazaniu danych innym administratorom, w szczególności spoza resortu obrony narodowej (np. na potrzeby ZUS).

W art. 38 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2016 r. poz. 1318) proponuje się dodać przepis zgodnie z którym, do przetwarzania danych osobowych, o których mowa w ust. 1, przepisów art. 13-22 rozporządzenia 2016/679 nie stosuje się w zakresie, w jakim dane te są niezbędne do zapewnienia prawidłowej realizacji zadań, o których mowa w art. 5 ust. 1 oraz art. 6 ust. 1.

W zakresie swojej właściwości SKW i SWW mogą zbierać, także niejawnie, wszelkie dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 27 i 28 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), a także korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je, w rozumieniu ustawy o ochronie danych osobowych, bez wiedzy i zgody osoby, której te dane dotyczą.

W zakresie realizacji zadań ustawowych SKW i SWW, o których mowa odpowiednio w art. 5 ust. 1 i art. 6 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego stosowanie przepisów rozporządzenia unijnego powinno być wyłączone. Jednocześnie, w zakresie danych osobowych przetwarzanych w związku z realizacją innych zadań, dopuszczalne wydaje się stosowanie, w ograniczonym zakresie, przepisów tego rozporządzenia. Każda jednak aktywność powinna być przy tym analizowana odrębnie, jak również zakres ewentualnego stosowania przepisów tego rozporządzenia do danych osobowych przetwarzanych w związku z daną aktywnością powinien być określany odrębnie w sposób zapewniający bezpieczeństwo realizacji wszystkich zadań w pełnym zakresie funkcjonowania.

3. Ustawa z dnia 19 czerwca 1974 r. – Kodeks pracy

Zmiany zaproponowane w Kodeksie pracy mają na celu przede wszystkim dostosowanie brzmienia obowiązujących przepisów prawa pracy do art. 6 ust. 1 lit c. rozporządzenia 2016/679 o ochronie danych, który wprowadził przesłankę istnienia „obowiązku prawnego" jako podstawy przetwarzania danych osobowych. Wskazana przesłanka stanowi główną podstawę legalizującą przetwarzanie danych osobowych pracowników lub kandydatów do pracy.

Przepisy rozporządzenia 2016/679 o ochronie danych przyznają państwom członkowskim swobodę, w określeniu zasad przetwarzania przez pracodawców danych osobowych pracowników, w tym poprzez uzależnienie ich gromadzenia od wyrażenia zgody osoby ubiegającej się o zatrudnienie bądź pracownika. Nowe brzmienie przepisów Kodeksu pracy w Art. 22^1 § 1 i 2 wskazuje na kategorie danych osobowych, które są niezbędne do pozyskania przez pracodawcę w związku z podejmowaniem przez niego działań przed zawarciem umowy o pracę oraz po jej zawarciu. W związku z tym, pracodawca może żądać ich udostępnienia przez pracownika.

Gromadzenie pozostałych kategorii danych osobowych osoby ubiegającej się o zatrudnienie lub pracownika uzależnione zostało od pozyskania na to dobrowolnej zgody, złożonej w postaci papierowej lub elektronicznej. Wyjątkiem w tym zakresie, jest pozyskanie przez pracodawcę danych osobowych biometrycznych, które mogą być pozyskane na podstawie udzielonej uprzednio, dobrowolnej zgody wyłącznie od pracownika. Brak jest bowiem uzasadnienia, dla pozyskiwania danych biometrycznych od osób ubiegających się o zatrudnienie. W wielu przypadkach, gromadzenie danych biometrycznych uzasadnione jest

stosunkiem pracy a jednocześnie ich gromadzenie w żadnym zakresie nie stanowi ograniczenie praw i wolności osób, których dane dotyczą. Ich udostępnienie musi być bowiem w pełni dobrowolne, a w wielu przypadkach może wiązać się z korzyściami dla samych pracowników. Biometryczny dostęp do pomieszczeń jest bardzo często szybszy i bardziej skuteczny, niż za pośrednictwem innych form uwierzytelniania tożsamości. Jednocześnie, konieczne jest zapewnienie szczególnych warunków technicznych gromadzenia danych biometrycznych, które zawiera rozporządzenie wydane przez ministra właściwego do spraw informatyzacji. Należy jednak wyodrębnić kategorie danych osobowych, których przetwarzanie z uwagi na ich szczególny związek ze sferą intymności człowieka nie powinno nastąpić za zgodą. Należą do nich dane o nałogach, o stanie zdrowia, o życiu seksualnym lub orientacji seksualnej. Ich gromadzenie możliwe będzie więc wyłącznie w przypadkach, gdy jest to konieczne dla wypełnienia obowiązku wynikającego z przepisu prawa. Przepisy takie, mogą również zobowiązywać do gromadzenia innych kategorii danych, w tym danych biometrycznych, co wyłącza konieczność pozyskania zgody na ich gromadzenie. Dodatkowo, mając na względzie motyw 42, 43 i 155 ww. rozporządzenia oraz korzystając z możliwości wprowadzenia przez państwo członkowskie przepisów szczególnych dotyczących przetwarzania danych osobowych w zatrudnieniu (art. 88 ww. rozporządzenia), w przepisach prawa pracy wprowadzona została instytucja „monitoringu", jako szczególna forma przetwarzania danych osobowych pracowników.

4. Ustawa z dnia 21 grudnia 1978 r. o odznakach i mundurach

Na podstawie art. 4 ustawy z dnia 21 grudnia 1978 r. o odznakach i mundurach, uprawnienia do nadawania odznaki honorowej mogą wynikać z rozporządzeń lub decyzji odpowiednich organów. Podmioty uprawnione do nadania odznaki honorowej przetwarzają dane osobowe w celu nadania odznaki honorowej oraz co do zasady prowadzą ewidencje osób, którym odznaka honorowa została nadana. Przetwarzanie danych osobowych jest niezbędne do realizacji obowiązków nałożonych na podmioty uprawnione przez rozporządzenia bądź decyzje odpowiednich organów. Szczegółowy zakres danych osobowych przetwarzanych przez podmioty uprawnione do nadania odznaki honorowej na podstawie rozporządzenia wydanego zgodnie z art. 4 ust. 1, 2 lub ust. 4 ww. ustawy określony został przez organy ustanawiające odznakę w rozporządzeniach wydanych na podstawie art. 6 ust. 1 ww. ustawy.

5. Ustawa z dnia 26 stycznia 1982 r. – Karta Nauczyciela

W proponowanych zmianach ustawy z dnia 26 stycznia 1982 r. – Karta Nauczyciela, zgodnie z propozycją ministra właściwego do spraw kultury i dziedzictwa narodowego, uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań.

Z tego względu proponuje się wprowadzenie do ustawy - Karta Nauczyciela, przepisów określających obowiązki przetwarzania danych w związku z wykonywaniem określonych w tych ustawach zadań.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego w zakresie, w jakim sprawuje nadzór nad szkolnictwem artystycznym, inne jednostki nadzoru nad tym szkolnictwem, szkoły i placówki artystyczne jako podmioty publiczne narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, zobowiązując zarazem administratora danych do umieszczenia na swojej internetowej stronie podmiotowej lub w Biuletynie Informacji Publicznej komunikatu o zaistniałym naruszeniu nie później niż 72 godziny od stwierdzenia naruszenia. Wprowadzenie ograniczeń praw określonych w art. 13 i 14 (prawo do informacji) oraz obowiązku, o którym mowa w art. 5 ust. 2 rozporządzenia 2016/679 (dokumentowanie przestrzegania przepisów o ochronie danych) jest konieczne nie tylko z uwagi na nadmierny koszt ale również inne niewspółmierne nakłady.

Należy podkreślić, że administrator byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach i włączeniach na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

Zmiana dokonywana w art. 85 w ust. 4 ma charakter porządkowy i polega na usunięciu odesłania do art. 7 ust. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

6. Ustawa z dnia 26 maja 1982 r. – Prawo o adwokaturze, ustawa z dnia 6 lipca 1982 r. o radcach prawnych, ustawa z dnia 5 lipca 2002 r. o świadczeniu przez prawników zagranicznych pomocy prawnej w Rzeczypospolitej Polskiej, ustawa z dnia 14 lutego 1991 r. – Prawo o notariacie, ustawa z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego i ustawa z dnia 15 czerwca 2007 r. o licencji doradcy restrukturyzacyjnego

Przepisy rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE dotyczą w dużej mierze zadań wykonywanych przez samorządy zawodowe adwokatów, radców prawnych, notariuszy i komorników oraz Ministra Sprawiedliwości na podstawie obowiązujących ustaw:

1) z dnia 26 maja 1982 r. – Prawo o adwokaturze;

2) z dnia 6 lipca 1982 r. o radcach prawnych;

3) z dnia 5 lipca 2002 r. o świadczeniu przez prawników zagranicznych pomocy prawnej w Rzeczypospolitej Polskiej;

4) z dnia 14 lutego 1991 r. – Prawo o notariacie;

5) z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji;

6) z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego;

7) z dnia 15 czerwca 2007 r. o licencji doradcy restrukturyzacyjnego.

Powyższe ustawy nie przewidują regulacji związanych z ochroną danych osobowych, jednak określają zadania publiczne, prowadzące do gromadzenia i przetwarzania takich danych, w związku z czym w świetle nowych regulacji prawa Unii Europejskiej zajdzie konieczność wprowadzenia stosownych przepisów ustawowych, w których zostaną określone ograniczenia zakresu obowiązków i praw wynikających z rozporządzenia 2016/679.

Wyłączenia znajdują umocowanie w art. 23 ust. 1 rozporządzenia 2016/679: częściowo w lit. e (ważne cele leżące w ogólnym interesie publicznym), częściowo w lit. g (zapobieganie naruszeniom zasad etyki w zawodach regulowanych, prowadzenie postępowań w takich

sprawach, ich wykrywanie oraz ściganie) oraz częściowo w lit. h (funkcje kontrolne i regulacyjne związane ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. e oraz g).

Zastosowanie podstawy derogacyjnej zawartej w art. 23 ust. 1 lit. e rozporządzenia 2016/679 w odniesieniu do samorządów zawodowych, ich organów i przedstawicieli znajduje uzasadnienie w przepisie art. 17 ust. 1 Konstytucji Rzeczypospolitej Polskiej, który stanowi, że w drodze ustawy można tworzyć samorządy zawodowe, reprezentujące osoby wykonujące zawody zaufania publicznego i sprawujące pieczę na należytym wykonywaniem tych zawodów w granicach interesu publicznego i dla jego ochrony. Umieszczenie tego przepisu w pierwszym rozdziale Konstytucji RP zatytułowanym „Rzeczpospolita" świadczy o zaliczeniu przez ustawodawcę normy z niego wynikającej do zasad ustrojowych.

Samorządy zawodowe są publicznymi korporacjami, a więc zrzeszeniami, czy też wspólnotami opartymi na więziach zawodowych. Z art. 17 ust. 1 Konstytucji RP wynikają funkcje samorządów zawodowych, do których prawidłowego wykonywania niezbędne jest wyposażenie ich w stosowne ustawowe kompetencje. Funkcje te obejmują reprezentację osób wykonujących dany zawód oraz sprawowanie pieczy nad jego należytym wykonywaniem w granicach interesu publicznego i dla jego ochrony. W tym kontekście Trybunał Konstytucyjny stwierdził, że „piecza" samorządów zawodów zaufania publicznego nad należytym wykonywaniem tych zawodów ma charakter działalności (funkcji) o cechach władztwa publicznego (wyrok TK z 18 lutego 2004 r., sygn. akt P 21/02).

Stąd też usprawnienie wykonywania zadań samorządów i związanych z nimi kompetencji nadzorczych Ministra Sprawiedliwości służy właściwemu wypełnianiu zasady prymatu interesu publicznego, wynikającej bezpośrednio ze wskazanej normy konstytucyjnej. Dotyczy to również postępowań administracyjnych skutkujących nabyciem bądź utratą uprawnień do wykonywania zawodu zaufania publicznego, wszczynanych zarówno na wniosek jak i z urzędu (m.in. o powołanie na stanowisko notariusza, cofnięcie licencji doradcy restrukturyzacyjnego). W tych przypadkach wskazać należy na istotny interes publiczny, polegający na konieczności sprawnego wykluczenia wykonywania uprawnień publicznoprawnych przez osoby, które w sposób określony obowiązującymi przepisami nimi utraciły przymiot dawania rękojmi należytego ich wykonywania.

Podkreślenia wymaga, że funkcje kontrolne Ministra Sprawiedliwości wobec zawodów zaufania publicznego (adwokata, radcy prawnego czy notariusza) nie ograniczają się jedynie do nadzoru nad prawidłowym wykonywaniem tych zawodów, ale także obejmują także proces dochodzenia do tych zawodów, stąd też, w ramach przesłanki określonej w art. 23 ust. 1 pkt e i h rozporządzenia 2016/679 celowe jest ograniczenie stosowania tego rozporządzenia zarówno przez Ministra Sprawiedliwości jak i powołane przez niego organy (m.in. komisje egzaminacyjne), a także organy samorządów zawodowych uczestniczące, z woli ustawodawcy, w tym procesie.

Zapobieganie naruszeniom zasad etyki w zawodach regulowanych, prowadzenie postępowań w takich sprawach, ich wykrywanie oraz ściganie (art. 23 ust. 1 pkt g rozporządzenia 2016/679) stanowi z kolei podstawę do wprowadzenia ograniczeń w przypadku przetwarzania danych osobowych przez adwokatów, radców prawnych czy notariuszy, w związku z dokonywanymi przez te podmioty czynnościami zawodowymi, prowadzonymi przeciwko nim postępowaniami dyscyplinarnymi jak również ma związek z ochroną tajemnicy zawodowej.

Zakres wprowadzonych ograniczeń proponuje się określić przez wymienienie expressis verbis przepisów rozporządzenia, których nie stosuje się w przypadku danych osobowych przetwarzanych w toku procedur ustawowych.

Proponuje się określić ograniczenia zakresu obowiązków wynikających z art. 13-15 ust. 1 i 3, 18, 19 i 21 rozporządzenia 2016/679, przez nowelizację ustawy – Prawo o adwokaturze, ustawy o radcach prawnych i adekwatnej (przez wprowadzenie odpowiedniego odesłania) ustawy o świadczeniu przez prawników zagranicznych pomocy prawnej w Rzeczypospolitej Polskiej, a także ustawy – Prawo o notariacie, ustawy o komornikach sądowych i egzekucji, ustawy o zawodzie tłumacza przysięgłego oraz ustawy o licencji doradcy restrukturyzacyjnego.

Proponowane ograniczenia wynikają z konieczności zapewnienia prawidłowego toku prowadzonych postępowań i ich sprawnego przebiegu oraz sprawnego wykonywania przez wymienione organy przypisanych im ustawowo zadań publicznoprawnych. Pozostaje to, co do zasady, w zgodzie z interesem indywidualnym osób, których dotyczą prowadzone postępowania wyrażającym się oczekiwaniem szybkiego przeprowadzenia poszczególnych postępowań administracyjnych, z których większość wszczynana jest na ich wniosek.

Jednocześnie, celowe i niezbędne dla ochrony osób, których dane osobowe są przetwarzane, wydaje się pozostawienie takich uprawnień jak prawo do żądania sprostowania danych osobowych (art. 16 rozporządzenia 2016/679) w sytuacji, gdy przepisy ustaw szczególnych nie regulują tej kwestii, czy prawo do przenoszenia danych osobowych (art. 20 rozporządzenia 2016/679).

Z uwagi na brzmienie art. 23 ust. 2 rozporządzenia 2016/679 nowelizacja wskazanych ustaw powinna określić cele przetwarzania i administratorów, dlatego też proponuje się wskazanie jako cel przetwarzania danych realizację ustawowych zadań, obowiązków lub uprawnień przez samorządy zawodowe adwokatów i radców prawnych oraz Ministra Sprawiedliwości, z jednoczesnym wskazaniem jako administratorów organów, którym są przypisane ustawowo zadania nadzorcze i kontrolne w ramach postępowań, wynikających z nowelizowanych ustaw oraz notariuszy, adwokatów i radców prawnych przetwarzających dane osobowe na potrzeby wykonywanego zawodu.

W celu wykonania dyrektyw zawartych w art. 23 ust. 2 lit. b, d i f rozporządzenia 2016/679 proponuje się wyraźne wskazanie, że wprowadzone wyłączenia stosuje się w przypadku danych osobowych niezbędnych do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień administratorów i podmiotów przetwarzających, dane osobowe podlegają zabezpieczeniom wynikającym z procedur prawnych, w których toku są przetwarzane oraz okres przechowywania danych osobowych ustala administrator zgodnie z celami ich przetwarzania, biorąc pod uwagę przepisy odrębne dotyczące terminów.

Jednocześnie należy wskazać, że charakter działań objętych wyłączeniem, w których są przetwarzane dane osobowe, minimalizuje potencjalne ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, stąd nie ma potrzeby dodatkowej regulacji określającej te ryzyka (art. 23 ust. 2 lit. g ogólnego rozporządzenia o ochronie danych). Nie ma również zastosowania dyrektywa zawarta w art. 23 ust. 2 lit. h ogólnego rozporządzenia o ochronie danych.

Ponadto proponuje się zastosowanie art. 90 rozporządzenia 2016/679 przez wprowadzenie regulacji, że w przypadku danych osobowych, które administrator lub podmiot przetwarzający otrzymali lub pozyskali w wyniku lub w ramach działania objętego obowiązkiem zachowania tajemnicy adwokackiej lub radcowskiej, notarialnej, tajemnicy tłumacza przysięgłego uprawnienia organu nadzorczego, o których mowa w art. 58 ust. 1 lit. e i f rozporządzenia 2016/679, zostają wyłączone.

7. Ustawa z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece

Zmiana w ustawie o księgach wieczystych i hipotece jest podyktowana koniecznością uregulowania w akcie prawnym rangi ustawy zakresu danych osób fizycznych, podlegających ujawnieniu w księdze wieczystej. Obecnie rodzaj danych osobowych wpisywanych w księgach wieczystych określa rozporządzenie Ministra Sprawiedliwości z dnia 15 lutego 2016 r. w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym (Dz. U. poz. 312, z późn. zm.). Zaproponowany w projektowanym art. 25 ust. 4 i art. 682 ust. 51 ustawy o księgach wieczystych i hipotece zakres danych jest identyczny jak ten określony w § 33 rozporządzenia w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym.

8. Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych

W związku z tym, że Generalny Inspektor ochrony Danych Osobowych w wyniku zmian wprowadzonych ustawą o ochronie danych osobowych stanie się Prezesem Urzędu Ochrony Danych Osobowych, a Biuro Generalnego Inspektora Ochrony Danych Osobowych przekształcone zostanie w Urząd Ochrony Danych Osobowych, konieczne stało się zastąpienie w ustawie z dnia 16 września 1982 r. o pracownikach urzędów państwowych, wyrazów „biuro generalnego Inspektora ochrony Danych Osobowych" wyrazami „Urząd Ochrony Danych Osobowych".

9. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach

Celem proponowanych wyjątków od rygorów ochrony danych osobowych jest z jednej strony wskazanie, że działalność archiwalna stanowi obowiązek w rozumieniu art. 6 ust. 1 lit c rozporządzenia 2016/679, z drugiej - zapewnienie możności korzystania z publicznych zasobów informacyjnych, w części stanowiącej państwowy zasób archiwalny w rozumieniu ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2016 r. poz. 1506 i 1948 oraz z 2017 r. poz. 1086). Ustawodawca uznał, że wolny dostęp do nich ma doniosłe znaczenie naukowe i kulturotwórcze, a przez to leży w interesie publicznym. Zasadne jest więc całkowite wyłączenie lub częściowe złagodzenie w tym zakresie wymogów ochronnych, których respektowanie na zasadach ogólnych wymagałoby niewspółmiernie dużego wysiłku i zaangażowania dużych kosztów po stronie jednostek państwowej sieci archiwalnej określonych w art. 22 unza albo wręcz uniemożliwiałoby udostępnianie składników państwowego zasobu archiwalnego zawierających chronione dane osobowe.

Argument niewspółmierności odnosi się również do obowiązku stosowania zasady rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679), informowania osób na podstawie art. 14 rozporządzeniem 2016/679, prawa do usunięcia danych na podstawie art. 17 rozporządzenia 2016/679 (w obu tych przepisach jest już zawarta możliwość ograniczeń w ramach działalności archiwalnej, ale propozycja ograniczenia dotyczy samej kwestii kosztów) oraz powiadamiania osób fizycznych na podstawie art. 34 rozporządzenia 2016/679 o ryzyku naruszenia ich wolności i praw w następstwie przetwarzania dotyczących ich danych osobowych. W przypadku archiwów historycznych należy wziąć pod uwagę, że dysponują one na ogół danymi wytworzonymi albo zebranymi w przeszłości przez inne podmioty. Skutkuje to dodatkowo faktyczną niemożnością komunikowania się z osobami, których dotyczą zarchiwizowane dane.

Ranga celów działalności archiwalnej przemawia ponadto za wyłączeniem prawa do sprzeciwu wobec przetwarzania danych, zastrzeżonego w art. 21 rozporządzenia 016/679. Zasoby archiwalne służą zachowaniu zbiorowej pamięci oraz wiedzy o przeszłości społeczeństwa i państwa – co również należy do sfery wolności i praw obywateli. Wobec tego pozostaje przyjąć w stosunku do nich środki ochrony inne niż wyłączenie przetwarzania danych. W obecnym stanie prawnym rodzaje dokumentacji o typowo sensytywnej zawartości informacyjnej podlegają np. karencjom dostępowym. Wyłączenie to jest dopuszczalne na podstawie art. 89 ust. 3 rozporządzenia 2016/679. Proponuje się także całkowite wyłączenie uprawnień, o których mowa w art. 16 oraz 18-20 rozporządzenia 2016/679. Zrezygnowano z wyłączenia art. 15 rozporządzenia 2016/679 (prawo dostępu do danych) oraz z możliwości ograniczenia korespondencji z podmiotem danych w tym zakresie. W pozostałym zakresie komunikacja z klientem zostałaby ograniczona w sposób wskazany w proponowanym art. 22c ust. 1.

Jednocześnie proponujemy w art. 22d wdrożenie w działalności archiwalnej odpowiednich środków zabezpieczenia, wymaganych przez art. 89 ust. 1 rozporządzenia 2016/679.

Do cech państwowego zasobu archiwalnego należy, że podlega on wieczystemu przechowywaniu przez podmioty inne niż te, które go wytworzyły albo zgromadziły, Materiały archiwalne stanowią historyczne świadectwo i zasługują na prawną ochronę przed zniszczeniem albo ingerencjami w ich treść.

Powyżej termin „cel archiwalny”, użyty w art. 89 ust. 3 rozporządzenia2016/679, utożsamiony został z terminem „działalność archiwalna”, zdefiniowanym przez art. 23 ustawy o narodowym

zasobie archiwalnym i archiwach (dalej jako „unza”). Jego zakres znaczeniowy obejmuje gromadzenie, ewidencjonowanie, przechowywanie, opracowywanie, zabezpieczenie i udostępnianie materiałów archiwalnych oraz prowadzenie działalności informacyjnej. Dodatkowo uwzględniono „cele archiwalne” związane z przetwarzaniem danych zawartych w dokumentacji innej niż materiały archiwalne.

Ma to znaczenie również w sferze nadzoru archiwów państwowych nad postępowaniem z dokumentacją w państwowych i samorządowych jednostkach organizacyjnych, w której to dokumentacji występować mogą dane osobowe. Archiwiści w toku wykonywanych kontroli mogą incydentalnie mieć wgląd również w dane osobowe, a brak takiej możliwości ograniczałby realizację ustawowych zadań. W celu uniknięcia pod tym względem niepewności prawnej, proponuje się treść art. 22 b ust. 3.

Proponuje się także odstąpienie od błędnego zobowiązania Naczelnego Dyrektora Archiwów Państwowych, w ustawie o narodowym zasobie archiwalnym i archiwach, do zabezpieczania danych osobowych w systemach teleinformatycznych eksploatowanych w podległych mu jednostkach organizacyjnych. Charakterystyka pojęcia „administrator” w art. 4 pkt 7 rozporządzenia 2016/679wskazuje bowiem na dyrektorów archiwów państwowych, którzy efektywnie decydują o celach i sposobach przetwarzania danych osobowych. Istotne jest przy tym, że archiwa państwowe stanowią odrębne jednostki organizacyjne i budżetowe, są tworzone w drodze rozporządzenia właściwego ministra i nie są zarządzane bezpośrednio przez Naczelnego Dyrektora Archiwów Państwowych. Z tego względu w przepisach zmieniających proponuje się modyfikację art. 21 ust. 1 pkt 10 oraz wyraźne wskazanie administratorów w art. 22b ust. 4.

Proponuje się także wprowadzenie uprawnienia dla podmiotów prowadzących działalność archiwalną do zlecania przetwarzania danych oraz przyjmowania takich zleceń od innych podmiotów.

10. Ustawa z dnia 21 marca 1985 r. o drogach publicznych

Projektowany art. 13fa wprowadza upoważnienia dla zarządów dróg, a jeśli nie zostały one powołane - dla zarządców dróg do przetwarzania danych osobowych w związku z poborem opłat za postój pojazdów samochodowych w strefie płatnego parkowania. Opłaty te są pobierane w interesie publicznym, ponieważ mają na celu zwiększenie rotacji parkujących pojazdów samochodowych lub realizację lokalnej polityki transportowej. W ust. 2 projektowanego przepisu ustalono zakres przetwarzanych danych osobowych, który zawiera

wyłącznie dane niezbędne dla prawidłowej egzekucji obowiązku, o którym mowa w art. 13 ust. 1 pkt 1 ustawy o drogach publicznych.

W art. 13hd ustawy o drogach publicznych proponuje się dodanie ust. 3a, na podstawie którego podmiot, któremu powierzony zostanie pobór opłaty elektronicznej, będzie również uprawniony do przetwarzania danych osobowych użytkowników dróg ponoszących tę opłatę. Szczegółowe uzasadnienie dla zaproponowanych w tym zakresie rozwiązań zostało przedstawione przy zmianach wprowadzanych w art. 18 ustawy.

Zmiana w art. 16i pkt 4 ma na celu jednoznaczne wskazanie, że obowiązkiem dostawcy Europejskiej Usługi Opłaty Elektronicznej (EETS) jest przekazywanie podmiotowi kontrolującemu prawidłowość uiszczenia opłaty elektronicznej danych osobowych użytkowników dróg naruszających obowiązek uiszczenia opłaty elektronicznej. Przedmiotowe rozwiązanie ma na celu zapewnienie możliwości efektywnego sprawowania przez Inspekcję Transportu Drogowego ustawowych zadań dotyczących kontroli prawidłowości uiszczenia ww. opłaty w sytuacji, gdy na terytorium RP będzie świadczona usługa EETS.

W art. 17 przewiduje się dodanie ust. 3 i 4, na podstawie których minister właściwy do spraw transportu zostanie uprawniony do przetwarzania danych osobowych w zakresie, w którym jest to niezbędne do realizacji niektórych nałożonych na niego ustawą obowiązków. Po pierwsze, zgodnie z art. 16f ust. 1 ustawy o drogach publicznych, ww. minister prowadzi rejestr EETS, do którego wpisani mogą zostać przedsiębiorcy mający siedzibę na terytorium RP, zamierzający świadczyć usługę EETS.

W dokumentach przedkładanych ministrowi przez potencjalnego dostawcę EETS znajdą się dane osobowe audytora oceniającego plan zarządzania ryzykiem wiązany ze świadczeniem usługi EETS oraz dane osobowe członków władz podmiotu składającego wniosek o wpis do rejestru. Zakres przetwarzanych danych ustalono w oparciu o brzmienie art. 35 pkt 1 ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2016 r. poz. 687, z późn. zm.), który określa jakie dane w odniesieniu do osób fizycznych (np. członków władz osób prawnych podlegających wpisowi do KRS) umieszcza się w Krajowym Rejestrze Sądowym. Po drugie, minister właściwy do spraw transportu jest odpowiedzialny za wydawanie oraz przedłużanie certyfikatów audytorów bezpieczeństwa ruchu drogowego (art. 24n ust. 5 i 7 ustawy o drogach publicznych). Oznacza to konieczność przetwarzania danych osobowych osób, które składają wnioski o wydanie lub przedłużenie ww. certyfikatu. Szeroki

zakres danych, które są przetwarzane przez ministra właściwego do spraw transportu wynika z faktu, że wnioskodawca musi wykazać, że nie został skazany prawomocnym wyrokiem sądu za umyślne przestępstwo lub umyślne przestępstwo skarbowe, co oznacza konieczność przedstawienia zaświadczenia z Krajowego Rejestru Karnego. Po trzecie, minister właściwy do spraw transportu powołuje i obsługuje Komisję, o której mowa w art. 16z ust. 1 ustawy o drogach publicznych, której zadaniem jest wydawanie opinii w sprawie sporów związanych z usługa EETS. Minister powołuje Komisje w drodze zarządzenia, przechowuje dokumentację pracy Komisji oraz zapewnia jej obsługę organizacyjno-biurową. W ramach realizacji ww. obowiązków minister będzie przetwarzał dane osobowe członków Komisji oraz osób, które, na żądanie Komisji, złożą informacje związane z istotą sporu. Zakres danych podlegających przetworzeniu ustalono w sposób wąski, niezbędny dla prawidłowej realizacji zadań przez ministra właściwego do spraw transportu.

Zmiany wprowadzane w art. 18 ustawy o drogach publicznych mają na celu upoważnienie Generalnego Dyrektora Dróg Krajowych i Autostrad (GDDKiA) do przetwarzania danych osobowych w związku z funkcjonowaniem systemów transportowych na drogach krajowych, a także zapewnienie odpowiednim służbom państwowym dostępu do tych danych na potrzeby realizacji ich obowiązków ustawowych. GDDKiA jest właścicielem elektronicznego systemu poboru opłat viaTOLL, któremu podlegają pojazdy ciężkie, systemu poboru opłat za przejazd autostradą, który dotyczy pojazdów lekkich oraz systemu wag preselekcyjnych, który ma za zadanie kontrolę czy drogami krajowymi nie poruszają się pojazdy przeciążone. Przedmiotowe systemy działają w związku z realizacją przez GDDKiA obowiązków ustawowych, do których należy pobór opłaty elektronicznej i opłaty za przejazd autostradą, a także przeciwdziałanie niszczeniu dróg. Są to więc działania podejmowane w interesie publicznym i w takim też celu konieczne jest przetwarzanie przez GDDKiA danych osobowych w związku z funkcjonowaniem wymienionych systemów transportowych na drogach krajowych.

Z technicznego punktu widzenia przedmiotowe systemy składają się z szeregu urządzeń, które umożliwiają przetwarzanie tych samych informacji wejściowych na dane wyjściowe w różnej formie i różnym zakresie, stosownie do potrzeb odbiorców końcowych. Systemy mogą raz zebrane dane wykorzystywać wielokrotnie na potrzeby GDDKiA oraz innych organów, głównie w celu monitorowania przewozu. Znaczna część danych zbieranych przez ww. systemy jest nie tylko niezbędna do wykonywania zadań ustawowych przez

GDDKiA, ale jest również pomocna dla służb nadzorujących przestrzeganie prawa, w tym Służby Celnej, organów kontroli skarbowej, Policji, Inspekcji Transportu Drogowego, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, gdyż są przez nie wykorzystywane do realizacji nałożonych na nich zadań ustawowych, w tym prowadzenia postępowań administracyjnych, karnych, wykroczeniowych, karno-skarbowych, a także prac statystycznych. Wraz z rozwojem systemów informatycznych w działalności operacyjnej poszczególnych służb, pojawiają się jednak nowe potrzeby na pozyskiwanie coraz większej liczby różnego rodzaju danych, które następnie są przez te służby wykorzystywane dla coraz efektywniejszego wypełniania swoich zadań, do których zaliczyć należy m.in. nadzór nad przestrzeganiem przepisów ruchu drogowego, rozwiązywanie spraw kryminalnych, ochronę granic państwa, nadzór nad realizacją dochodów z podatków. Stąd wynika coraz większa liczba wniosków o umożliwienie automatycznego dostępu do danych GDDKiA dla celów operacyjnych prowadzonych przez funkcjonariuszy ww. służb, dlatego też są one bardzo zainteresowane zacieśnianiem współpracy w tym zakresie. W związku z przyrostem wniosków o przekazanie danych, należy stworzyć rozwiązania prawne na szczeblu ustawowym umożliwiające gromadzenie i przetwarzanie danych przez GDDKiA pozyskiwanych w związku z funkcjonowaniem systemów poboru opłat oraz systemów ważenia pojazdów, a także zinformatyzowanie wymiany informacji pomiędzy systemami transportowymi GDDKiA a właściwymi organami państwa. Zaproponowane zmiany w art. 18 ustawy o drogach publicznych wpłyną na poprawę efektywności działania organów aparatu administracji publicznej, a także na obniżenie kosztów funkcjonowania systemów informatycznych, obsługujących każdą z instytucji współpracujących.

Mając powyższe na względzie, w art. 18 ustawy o drogach publicznych proponuje się dodanie ust. 2a, który wprowadzi jednoznaczne upoważnienie dla przetwarzania danych, w tym danych osobowych, przez GDDKiA w zakresie niezbędnym dla zadań ustawowych realizowanych bezpośrednio przez ten organ. Zakres gromadzenia i przetwarzania danych ograniczono do tych zadań, w których wykonywanie tych czynności jest rzeczywiście niezbędne. Uzyskane dane będą mogły być wykorzystywane przy wykonywaniu ściśle określonych ustawowych zadań GDDKiA, a także udostępniane odpowiednim upoważnionym organom państwowym.

W projektowanym ust. 2b szczegółowo określono zakres danych osobowych, które będą przetwarzane w związku z koniecznością wykonywania poszczególnych obowiązków

ustawowych nałożonych na GDDKiA. W celu realizacji zadania polegającego na poborze opłat za przejazd autostradą przetwarzane będą dane konieczne do wystawiania wezwań do zapłaty, w sytuacji gdy użytkownik autostrady nie uiszcza opłaty za przejazd w Miejscu Poboru Opłat. W celu realizacji zadania polegającego na poborze opłaty elektronicznej konieczne jest przetwarzanie przez GDDKiA danych osobowych w związku z umowami zawieranymi z użytkownikami korzystającymi z dróg krajowych lub ich odcinków, na których pobiera się tę opłatę. Dane zebrane w tym zakresie są konieczne do prawidłowej identyfikacji użytkownika w ramach realizowanego procesu pobierania opłaty elektronicznej. Dane te umożliwiają również weryfikację tożsamości użytkownika podczas dokonywania wszelkich czynności w ramach umowy z GDDKiA (modyfikacja konta, doładowanie konta, zamknięcie umowy, dopisanie pojazdu do konta), a także są niezbędne do zapewnienia prawidłowości procesów związanych z naliczaniem opłaty elektronicznej (w tym weryfikacji czy opłata została naliczona w należytej wysokości). Oprócz tego gromadzone i przetwarzane są dane tych użytkowników, którzy zostali zidentyfikowani jako osoby naruszające obowiązek uiszczenia opłaty elektronicznej. W celu realizacji zadań z zakresu przeciwdziałania niszczeniu dróg krajowych przez ich użytkowników przetwarzaniu podlegać będą dane w postaci obrazu pojazdu, jego numeru rejestracyjnego oraz dane umożliwiające określenie miejsca i czasu przemieszczenia się na pojazdu na sieci dróg krajowych. Dane te są zbierane przez urządzenia systemu wag preselekcyjnych (m. in. kamery) i mają na celu zidentyfikowanie użytkowników dróg, którzy poruszają się drogami krajowymi pojazdami przeciążonymi, niezgodnie z obowiązującymi przepisami prawa.

W ust. 2c ustawy ustalono okres, przez który mogą być przechowywane dane osobowe, o których mowa w ust. 2a. Co do zasady termin ten będzie wynosić nie dłużej niż 12 miesięcy. Wyjątkiem będą sytuacje, w których dane osobowe są niezbędne do prowadzenia postępowania administracyjnego, sądowego lub egzekucyjnego albo dla zapewnienia prawidłowego wnoszenia opłat elektronicznych przez użytkowników dróg oraz ich rozliczania (zadanie GDDKiA polegające na poborze opłaty elektronicznej ma charakter ciągły, więc nie jest możliwe określenie terminu przetwarzania przez ten organ danych osobowych użytkowników dróg zarejestrowanych w elektronicznym systemie poboru opłat). W celu zapobieżenia konieczności zbyt długiego przechowywania danych przepis zobowiązuje GDDKiA do ich weryfikacji nie rzadziej niż co 3 miesiące, w celu oceny czy określona grupa danych jest rzeczywiście niezbędna do wykonywania przez GDDKiA zadań ustawowych.

Zgodnie z projektowanym ust. 2d do danych osobowych gromadzonych i przetwarzanych przez GDDKiA nie będą miały zastosowania art. 13 i 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Przepisy te nakładają na administratora danych obowiązek poinformowania danej osoby o zbieraniu dotyczących jej danych osobowych. Przedmiotowy obowiązek można wyłączyć na mocy art. 23 ww. rozporządzenia. Obowiązek ten należy wyłączyć w stosunku do danych określonych w projektowanym art. 18 ust. 2a, ponieważ zadania dla których realizacji niezbędne jest przetwarzanie danych osobowych przez GDDKiA obejmują pobór danin publicznych (opłat za przejazd) oraz przeciwdziałanie niszczeniu dróg, a więc zadania które są realizowane w ważnym ogólnym interesie publicznym, w tym ważnym interesie finansowym. Środki z opłat trafiają do Krajowego Funduszu Drogowego, z którego realizowane są inwestycje na drogach krajowych. Budowa dróg krajowych jest niewątpliwie zadaniem realizowanym w interesie publicznym, ponieważ ma istotny wpływ na bezpieczne przemieszczanie się obywateli po terytorium RP. Podobnie istotne jest zadanie polegające na przeciwdziałaniu niszczeniu dróg, które ma na celu zapobieżenie poruszaniu się drogami krajowymi pojazdów przeciążonych, które nie tylko niszczą nawierzchnię dróg (co oznacza konieczność wydatkowania środków publicznych na remonty dróg), lecz również bezpośrednio zagrażają bezpieczeństwu ruchu. Wyłączenie obowiązku informowania ma na celu umożliwienie GDDKiA skutecznego wykonywania jej zadań ustawowych. Brak takiego wyłączenia mógłby prowadzić do nadużyć ze strony użytkowników dróg, którzy na podstawie informacji uzyskanych od GDDKiA byliby w stanie zawczasu uniknąć kontroli prowadzonych przez zarządcę drogi, co niweczyłoby cele, dla których funkcjonują systemy poboru opłat za przejazd oraz system wag preselekcyjnych.

W ust. 2e wskazano zamknięty katalog służb i innych podmiotów, które będą miały dostęp do danych gromadzonych przez GDDKiA w zakresie niezbędnym do realizacji przez nie ustawowych zadań. W powyższym katalogu wymieniono służby i inne podmioty, które wykonują zadania istotne z punktu widzenia interesu publicznego, takie jak ochrona bezpieczeństwa państwa, ochrona bezpieczeństwa i porządku publicznego, ochrona ważnego interesu finansowego RP lub UE. Podkreślić w tym miejscu należy, że proponowane przepisy nie nakładają na GDDKiA obowiązku gromadzenia i przetwarzania danych, które nie są lub

nie mogą być pozyskiwane w związku z wykonywaniem zadań ustawowych przez ten organ. Wymaga podkreślenia, że rozwiązania zaproponowane w ust. 2e będą miały zastosowanie wyłącznie w przypadku, gdy odrębne przepisy, regulujące funkcjonowanie właściwych organów państwa, nie określają w inny sposób pozyskiwania przez nie danych. Intencją projektodawców nie jest bowiem w przedmiotowym zakresie wprowadzenie dodatkowych utrudnień dla podmiotów, które już pozyskują obecnie od GDDKiA w trybie pisemnym. Powinno więc to się odbywać na dotychczas obowiązujących zasadach uregulowanych w przepisach odrębnych. W ust. 2f określono przy tym jakie elementy składowe powinien zawierać pisemny wniosek o udostępnienie danych.

W projektowanych ust. 2g - 2i uregulowano tryb udostępniania danych znajdujących się w posiadaniu GDDKiA za pomocą środków komunikacji elektronicznej. Zaproponowane rozwiązanie ma na celu przede wszystkim usprawnienie wymiany danych poprzez umożliwienie ich przekazywania w trybie automatycznym. W tym przypadku zastosowano więc inną konstrukcję niż w zakresie udostępniania tych danych w trybie pisemnym. Zasadą więc będzie, że udostępnianie danych w trybie automatycznym będzie następować zgodnie z wprowadzanym art. 18 ust. 2g - 2i, a nie przepisami właściwych ustaw regulujących funkcjonowanie poszczególnych organów, służb i innych instytucji państwowej. Jako, że poszczególne ustawy ustrojowe w różny sposób regulują kwestię dostępu ww. podmiotów do danych za pośrednictwem środków komunikacji elektronicznej albo w ogóle nie przewidują tego typu rozwiązań, zasadnym jest wprowadzenie przepisu umożliwiającego niedyskryminacyjny dostęp wszystkim podmiotom wymienionym w projektowanym art. 18 ust. 2c, za pomocą środków komunikacji elektronicznej, na takich samych zasadach. W celu uzyskania danych w trybie automatycznym właściwe organy muszą spełniać dodatkowe warunki, które zostały wymienione w ust. 2h. Zasadą będzie pozyskiwanie danych za pomocą środków komunikacji elektronicznej wyłącznie w przypadku uzyskania stosownej zgody GDDKiA. Odrębne rozwiązanie przewidziano w projektowanym ust. 2i dla Agencji Bezpieczeństwa Wewnętrznego (ABW), ponieważ zgodnie z zasadą wyrażoną w art. 34 ust. 2a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2016 r. poz. 1897) na administratorach zbiorów danych ciąży obowiązek udostępniania danych w trybie automatycznym Szefowi ABW.

W celu zapewnienia, że podmioty, który uzyskały dane od GDDKiA, nie przechowują ich przez czas dłuższy niż jest to niezbędne do realizacji ich ustawowych zadań wprowadzono w ust. 2j

zasadę, zgodnie z którą rzeczone podmioty dokonują weryfikacji danych, nie rzadziej niż co 3 miesiące od dnia ich uzyskania, usuwając dane zbędne.

W ustawie o drogach publicznych dodaje się również nowy art. 20h, który ma na celu upoważnienie zarządców dróg publicznych do przetwarzania danych osobowych w zakresie niezbędnym do realizacji ich ustawowych zadań. W ust. 1 uregulowano kwestię przetwarzania danych w celu realizacji zadań polegających na przeciwdziałaniu niszczeniu dróg przez użytkowników oraz dokonywaniu okresowych pomiarów ruchu drogowego.

W przedmiotowym zakresie odesłano do odpowiedniego stosowania do przepisów regulujących przetwarzanie danych osobowych przez GDDKiA oraz określających zasady ich udostępniania uprawnionym służbom i instytucjom państwowym. W ust. 2 wprowadzono uprawnienie dla zarządców dróg publicznych w celu realizacji zadań polegających na wydawaniu zgód na przebudowę lub remont obiektów budowlanych lub urządzeń istniejących w pasie drogowym niezwiązanych z gospodarka drogową lub obsługa ruchu, na umieszczenie nadziemnych urządzeń liniowych w odległości mniejszej niż 5 m od granicy pasa drogowego oraz na usytuowanie obiektu budowalnego i niebędących obiektami budowlanymi reklam w odległości mniejszej niż określona w art. 43 ust. 1 ustawy o drogach publicznych.

11. Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich

Dokonywana zmiana ma charakter dostosowujący. Po pierwsze, obowiązujące przepisy w zakresie ochrony danych osobowych - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) - zostaną uchylone. Odwołania zawarte w ustawie o Rzeczniku Praw Obywatelskich do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych musiały więc zostać dostosowane do nowej sytuacji prawnej.

Po drugie, art. 9 rozporządzenia 2016/679 wskazuje na przesłanki przetwarzania danych osobowych wrażliwych. Spośród wszystkich przewidzianych w rozporządzeniu, do Rzecznika Praw Obywatelskich mogłaby znaleźć zastosowanie - oprócz art. 9 ust. 2 lit. a, c, e lub f - również art. 9 ust. 2 lit. g, tj. gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego. Konstrukcja tej przesłanki może rodzić poważne wątpliwości interpretacyjne, czy norma kompetencyjna stanowiąca wyraźnie o przetwarzaniu danych musi znaleźć się w ustawie, czy też wystarczającym byłoby, by ustawa przewidywała zadanie, dla którego

realizacji konieczne jest przetwarzanie danych. Z tego względu, uwzględniając konieczność utrzymania dotychczasowych kompetencji Rzecznika Praw Obywatelskich do przetwarzania danych osobowych dla skutecznego wykonywania jego konstytucyjnych i ustawowych zadań, zdecydowano się wprowadzić przepis upoważniający do przetwarzania danych osobowych wrażliwych. Jednocześnie wskazano, że uprawnienie to znajduje zastosowanie wyłącznie w celu ochrony wolności i praw człowieka i obywatela i przy realizacji przez Rzecznika jego ustawowych zadań.

Uwzględniając powyższe, zmiana w art. 17c ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich związana jest po pierwsze z uchyleniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dotychczasowe brzmienie art. 17c ustawy o Rzeczniku Praw Obywatelskich przyznawało podstawę prawną do przetwarzania wszelkich danych osobowych, w tym danych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych niezbędnych do realizacji ustawowych zadań Rzecznika. Po drugie, zmiana wynika z brzmienia art. 9 rozporządzenia 2016/679.

12. Ustawa z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne

Wprowadzane zmiany mają cel doprecyzowujący. Ich istotą jest wskazanie celu przetwarzania danych osobowych.

13. Ustawa z dnia 7 września 1991 r. o systemie oświaty

W proponowanych zmianach ustawy z dnia 7 września 1991 r. o systemie oświaty zgodnie z propozycją ministra właściwego do spraw kultury i dziedzictwa narodowego, uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań.

Z tego względu proponuje się wprowadzenie do ustawy przepisów określających obowiązki przetwarzania danych w związku z wykonywaniem określonych w tych ustawach zadań.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego w zakresie, w jakim sprawuje nadzór nad szkolnictwem artystycznym, inne jednostki nadzoru nad tym szkolnictwem, szkoły i placówki artystyczne jako podmioty publiczne narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, zobowiązując zarazem administratora danych do umieszczenia na swojej stronie internetowej lub w Biuletynie Informacji Publicznej komunikatu o zaistniałym naruszeniu nie później niż 72 godziny od stwierdzenia naruszenia. Wprowadzenie ograniczeń praw określonych w art. 13 i 14 (prawo do informacji) oraz obowiązku, o którym mowa w art. 5 ust. 2 rozporządzenia 2016/679 (dokumentowanie przestrzegania przepisów o ochronie danych) jest konieczne nie tylko z uwagi na nadmierny koszt ale również inne niewspółmierne nakłady.

Należy podkreślić, że administrator byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach i włączeniach na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

Zmiana dokonywana w art. 92k w ust. 2 pkt 2 lit g ma charakter porządkowy i polega na usunięciu odesłania do art. 23 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

14. Ustawa z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej.

W proponowanej zmianie przepisów ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz. U. z 2017 r. poz. 862), uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679, zgodnie z którym przepis prawa krajowego powinien określać obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych.

W związku z powyższym w przepisach ustawy zaproponowano zmiany polegające na określeniu zakresu danych przetwarzanych w związku z przyznawaniem przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego odznak, nagród i stypendiów, prowadzeniem rejestru instytucji kultury, a także powoływaniem i odwoływaniem dyrektora instytucji kultury oraz powierzaniem pełnienia obowiązków dyrektora albo powierzaniem zarządzania instytucją kultury osobie fizycznej. Z tego samego powodu proponuje się wprowadzenie nowych przepisów określających obowiązek przetwarzania danych w związku z wykonywaniem określonych w ustawie zadań przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego, jednostki samorządu terytorialnego oraz instytucje kultury. Obowiązek ten dotyczy także przetwarzania danych w związku z wszelkiego typu dofinansowaniem działalności kulturalnej w ramach mecenatu państwa nad działalnością kulturalną.

Jednocześnie proponuje się wskazanie 80-letniego okresu przechowywania danych osobowych w związku z nadaniem odznaki honorowej „Zasłużony dla Kultury Polskiej” i nadaniem Medalu „Zasłużony Kulturze Gloria Artis” oraz 5-letniego 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. W pozostałym zakresie okres przetwarzania danych byłby zależny od realizacji celu przetwarzania.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom ponoszonym w związku ze sporządzeniem odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego, jednostka samorządu terytorialnego oraz instytucja kultury, jako podmioty publiczne, których działalność finansowana jest ze środków budżetowych narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, poprzez wprowadzenie normy nakazującej nie później niż 72 godziny od stwierdzenia naruszenia, umieszczenie komunikatu na stronie podmiotowej w

Biuletynie Informacji Publicznej lub na stronie internetowej. Prawa określone w art. 13 i 14 (prawo do informacji) rozporządzenia 2016/679 również byłyby ograniczone w takim zakresie, w jakim są niezbędne do realizacji zadań ustawowych administratora tych danych. Należy podkreślić, że administrator danych osobowych byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach.

15. Ustawa z dnia 16 października 1992 r. o orderach i odznaczeniach

Na podstawie art. 2 ustawy z dnia 16 października 1992 r. o orderach i odznaczeniach, ordery i odznaczenia nadaje Prezydent Rzeczypospolitej Polskiej z własnej inicjatywy lub na wniosek innych instytucji lub organów. W celu realizacji obowiązków wynikających z ustawy niezbędne jest przetwarzanie danych osobowych osób ubiegających się o nadanie orderu lub odznaczenia. Informacje dotyczące rodzaju danych osobowych przetwarzanych przez Prezydenta oraz uprawnione osoby są określone w rozporządzeniu wydanym na podstawie art. 9 ustawy. Wniosek o nadanie orderu lub odznaczenia powinien zawierać szczegółową informacje o zasługach i osiągnięciach osoby, której dotyczy, w szczególności niezbędne jest wykazanie zasług po otrzymaniu ostatniego orderu lub odznaczenia.

16. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych

W projektowanych zmianach ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679 (określającego podstawę przetwarzani danych osobowych), który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz wskazywał rodzaj przetwarzanych danych osobowych.

Z tego względu zaproponowano zmiany określające zakres danych przetwarzanych w związku z wynagrodzeniem z tytułu tzw. public lendingrights, a także wprowadzenie nowych przepisów określających obowiązek przetwarzania danych w związku z wykonywaniem określonych w ustawie zadań przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego oraz organizacje zbiorowego zarzadzania.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy.

Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i dziedzictwa narodowego oraz organizacja zbiorowego zarzadzania jako podmioty publiczne narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzeniem 2016/679, z jednoczesnym zobowiązaniem do publicznego poinformowania na stronie podmiotowej w BIP lub internetowej stronie podmiotowej, o naruszeniu ochrony w ciągu 72 godzin od jego stwierdzenia. Prawo określone w art.14 rozporządzeniem 2016/679 (prawo do informacji) również byłyby ograniczone w takim zakresie, w jakim są niezbędne do realizacji zadań ustawowych administratora danych osobowych. Należy podkreślić, że administrator byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach poprzez umieszczenie stosownej informacji na stronie BIP.

17. Ustawa z dnia 14 marca 1994 r. o zakładowym funduszu świadczeń socjalnych

Zaproponowane zmiany mają na celu przede wszystkim dostosowanie brzmienia obowiązujących przepisów do art. 6 ust. 1 lit c. rozporządzenia 2016/679 o ochronie danych, który wprowadził przesłankę istnienia „obowiązku prawnego” jako podstawy pobierania danych osobowych.

Zgodnie z projektowaną regulacją 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, obejmujących: imię i nazwisko, datę urodzenia, stopień pokrewieństwa, adres zamieszkania, a także innych danych osobowych tych osób, jeżeli podanie takich danych jest niezbędne do ustalenia sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej. Wyrażenie zgody następuje w oświadczeniu złożonym w postaci papierowej lub elektronicznej.

18. Ustawa z dnia 24 czerwca 1994 r. o własności lokali

Wprowadzana zmiana ma charakter doprecyzowujący. Jej istotą jest wskazanie na rolę ujętego w nim podmiotu jako na administratora danych.

19. Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego

Dla systemowej spójności w wyniku zmian dokonywanych w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta konsekwentnie należy dokonać zmiany w ustawie o ochronie zdrowia psychicznego w zakresie organu obowiązanego do ochrony praw osób korzystających ze świadczeń zdrowotnych udzielanych przez szpital psychiatryczny (art. 10b ust. 1 ww. ustawy).

Zmiana ww. ustawy dotyczy przetwarzania danych osobowych przez Rzeczników Praw Pacjenta Szpitala Psychiatrycznego w ramach przysługujących im uprawnień. W celu realizacji określonych zadań Rzecznik Praw Pacjenta Szpitala Psychiatrycznego ma prawo między innymi do wglądu w dokumentację medyczną za zgodą pacjenta, jego przedstawiciela ustawowego, opiekuna prawnego lub faktycznego. Zaznaczyć przy tym należy, ze zgodnie z § 3 rozporządzenia Ministra Zdrowia z dnia 13 stycznia 2006 r. w sprawie szczegółowego trybu i sposobu działania Rzecznika Praw Pacjenta Szpitala Psychiatrycznego, Rzecznik Praw Pacjenta Szpitala Psychiatrycznego z własnej inicjatywy dokonuje oceny przestrzegania praw pacjenta, w szczególności w odniesieniu do pacjentów:

1) przyjętych do szpitala psychiatrycznego bez zgody;
2) wobec których zastosowano przymus bezpośredni;
3) niezdolnych do wyrażenia zgody lub stosunku do przyjęcia albo leczenia;
4) przebywających w szpitalu psychiatrycznym na mocy orzeczenia sądowego o zastosowaniu środka zabezpieczającego.

Zatem dla realizacji ww. zadań - z własnej inicjatywy - konieczne jest wyposażenie Rzeczników w uprawnienie dostępu do dokumentacji medycznej, bez zgody ww. osób.

20. Ustawa z dnia 27 października 1994 r. o autostradach płatnych oraz o Krajowym Funduszu Drogowym

W ustawie o autostradach płatnych oraz o Krajowym Funduszu Drogowym zachodzi konieczność nowelizacji art. 63d, który reguluje kwestię kontroli budowy i eksploatacji autostrady w zakresie przestrzegania warunków umowy o budowę i eksploatację autostrady. Jako, że osoby kontrolujące mogą żądać pisemnych lub ustnych wyjaśnień mających związek z przedmiotem kontroli wprowadzono upoważnienie dla podmiotów kontrolnych do gromadzenia i przetwarzania danych osobowych osób, które złożyły wyjaśnienia (por. projektowany art. 63d ust. 3). Zakres danych, które będą przetwarzane w powyższym zakresie ustalono w dodawanym w ust. 4, który zostanie dodany w art. 64d.

21. Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli

Zmiana o charakterze dostosowującym. W związku z tym, że Generalny Inspektor Ochrony Danych Osobowych w wyniku zmian wprowadzonych ustawą o ochronie danych osobowych stanie się Prezesem Urzędu Ochrony Danych Osobowych, a Biuro Generalnego Inspektora Ochrony Danych Osobowych przekształcone zostanie w Urząd Ochrony Danych Osobowych, konieczne stało się zastąpienie w ustawie wyrazów „Generalny Inspektor Ochrony Danych Osobowych" wyrazami „Prezes Urzędu Ochrony Danych Osobowych".

22. Ustawa z dnia 5 stycznia 1995 r. o fundacji – Zakład Narodowy imienia Ossolińskich.

W proponowanych zmianach ustawy z dnia 5 stycznia 1995 r. o fundacji - Zakład Narodowy imienia Ossolińskich (Dz. U. poz. 121, z późn. zm.) uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679, który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych przetwarzanych w ramach zadań przypisanych ustawą. Zagadnienie to uregulowano w dodawanych przepisach art. 5 ust. 2, art. 12 ust. 2a, art. a5 ust. 2a.

Na podstawie art. 23 rozporządzeniem 2016/679 proponuje się ograniczenie niektórych praw podmiotu danych, o których mowa w rozporządzeniu 2016/679. Wynika to z charakteru Zakładu, którego głównymi celami działalności są:

1) utrzymywanie Narodowej Biblioteki Ossolineum i pomnażanie jej zbiorów, zwłaszcza w zakresie humanistyki polskiej i słowiańskiej, oraz ich opracowywanie i upowszechnianie,
2) utrzymywanie Muzeum Książąt Lubomirskich i pomnażanie jego zbiorów w zakresie sztuki i pamiątek historycznych oraz ich opracowywanie i upowszechnianie,
3) wspieranie i prowadzenie prac naukowo-badawczych,
4) działalność wydawnicza.

Działalność ta nie jest bezpośrednio związana z przetwarzaniem danych osobowych, choć Zakład niewątpliwie takimi dysponuje i są one niezbędne do realizacji zadań nałożonych ustawą. Brak proponowanych ograniczeń spowodowałby konieczność zaangażowania nadmiernych kosztów, czasu i działań.

Proponuje się zatem ograniczenie praw podmiotów danych, o których mowa w art. 12 i 15 rozporządzeniem 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych.

Propozycja jest uzasadniona 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. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzeniem 2016/679, wprowadzając normę nakazującą umieścić na stronie podmiotowej Biuletynu Informacji Publicznej informację o zaistniałym naruszeniu w terminie 72 godzin od stwierdzenia naruszenia.

Prawa określone w art. 13-14 (prawo do informacji) oraz 17-19 rozporządzeniem 2016/679 również byłyby ograniczone z jednoczesnym nałożeniem na ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego i Zakład obowiązku zamieszczenia na stronie podmiotowej stosownej informacji o obowiązujących ograniczeniach i włączeniach. Proponuje się także, aby ww. podmioty mogły pełnić funkcję podmiotu przetwarzającego dane osobowe na zlecenie innego podmiotu lub zlecać przetwarzanie w jego imieniu danych osobowych.

23. Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej

Projektowana nowelizacja ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2016 r. poz. 1068, z późn. zm.), zwanej dalej „ustawą” lub „ustawą o statystyce publicznej”, ma przede wszystkim za zadanie dostosowanie przepisów ustawy do zasad przetwarzania danych osobowych, wprowadzonych przepisami rozporządzenia 2016/679.

W tym celu została dokonana analiza obowiązujących przepisów ustawy w zakresie zasad przetwarzania danych osobowych dla celów statystycznych, zawartych w rozdziale 4a ustawy oraz w jej przepisach ogólnych. W konsekwencji konieczne okazało się przeprowadzenie szeregu zmian, tak aby wprowadzone rozwiązania legislacyjne, wynikające z rozporządzenia 2016/679, były spójne i miały zastosowanie do całokształtu działań służb statystyki publicznej.

W przypadku statystyki publicznej dane osobowe stanowią część zbieranych, opracowywanych, gromadzonych i przechowywanych danych statystycznych. Dane osobowe, tak samo jak inne dane, z chwilą ich zebrania przez służby statystyki publicznej, stają się danymi statystycznymi i są objęte tajemnicą statystyczną. Tajemnica statystyczna jest określona w art. 10 ustawy i gwarantuje pełną poufność zebranych danych. To nie jedyne

rozwiązanie funkcjonujące na gruncie przepisów ustawy, które ma zastosowanie zarówno do danych niebędących danymi osobowymi, jak i danych osobowych zbieranych przez służby statystyki publicznej. Wszelkie mechanizmy określone w ustawie, takie jak: pozyskiwanie, gromadzenie, opracowywanie danych, uprawnienia i obowiązki odnoszą się do danych statystycznych, jako ogółu. Wobec czego, w pewnym zakresie mogą dotyczyć tej części danych, które są danymi osobowymi.

Zatem dostosowując przepisy ustawy do rozporządzenia 2016/679 konieczne stało się szersze ujęcie zmian. Wprowadzone zmiany obejmują: przepisy dotyczące przetwarzania danych osobowych, na które składają się zmiany w obowiązującym rozdziale 4a, w przepisach ogólnych, wprowadzenie dwóch nowych rozdziałów 2b i 5a, doprecyzowanie zadań Prezesa Głównego Urzędu Statystycznego oraz zmiany, które wynikają z zamieszczenia w ustawie przepisów projektowanej nowelizacji i polegają na dostosowaniu obowiązujących przepisów do projektowanych zmian.

W pkt 1 wprowadzającym zmiany w art. 2 ustawy o statystyce publicznej modyfikacji w stosunku do obecnie obowiązujących definicji uległy definicje danych statystycznych i operatu do badań statystycznych. Definicja osoby fizycznej prowadzącej działalność gospodarczą została przeniesiona z art. 42 ust. 2 ustawy. Wprowadzenie definicji niepublicznych systemów informacyjnych wynika ze wskazania tych systemów jako jednego ze źródeł danych, z których statystyka publiczna zbiera dane w celu realizacji zadań ustawowych. Związane jest to również z faktem, że zgodnie z obowiązującym art. 13 ust. 5 i art. 18 ust. 3 służby statystyki publicznej są obowiązane do wykorzystywania danych już zgromadzonych i przechowywanych w istniejących rejestrach i systemach informacyjnych prowadzonych przez różnego rodzaju podmioty i organy. W przypadku niepublicznych systemów informacyjnych, jest to wskazanie tych rejestrów, ewidencji i baz danych, które zawierają istotne dane z punktu widzenia prowadzonych przez służby statystyki publicznej prac. Przyjęta na gruncie ustawy konstrukcja przepisów jest analogiczna do konstrukcji rejestrów urzędowych i systemów informacyjnych administracji publicznej i składa się z: definicji (projektowany pkt 15 w art. 2 ustawy), wskazania tych systemów wśród źródeł pozyskiwania danych (projektowane - art. 5a ust. 2 i art. 35c ust. 2 ustawy). Zakłada się, że dane z tych systemów będą przekazywane bezpłatnie, podobnie jak ma to miejsce w przypadku rejestrów urzędowych i systemów informacyjnych administracji publicznej.

Natomiast zrezygnowano z nakładania na podmioty prowadzące te systemy administracyjne obowiązku, o którym mowa w art. 13 ust. 3 ustawy, tj.:

1) stosowania standardów klasyfikacyjnych, numeru identyfikacyjnego i oznaczeń kodowych przyjętych w rejestrze terytorialnym, o których mowa w rozdziale 6;

2) przekazywania, na wniosek Prezesa Głównego Urzędu Statystycznego, informacji o zawartości informacyjnej eksploatowanych systemów informacyjnych administracji publicznej oraz rejestrów urzędowych;

3) informowania Prezesa Głównego Urzędu Statystycznego o projektowanym zakresie informacyjnym systemów informacyjnych administracji publicznej oraz rejestrów urzędowych na etapie ich tworzenia lub modernizacji.

U podstaw wykorzystania danych zgromadzonych w niepublicznych systemach informacyjnych leży zasada maksymalnego wykorzystania danych już przetwarzanych w systemach dla innych celów niż cele statystyczne statystyki publicznej i tym samym stałe dążenie do redukowania, do niezbędnego minimum, obciążeń respondentów przekazywaniem określonych danych bezpośrednio służbom statystyki, jak również obciążeń administracyjnych. Pozyskiwanie danych z tych systemów może wpłynąć na znaczną poprawę jakości badania przy ograniczeniu jego kosztów i ograniczeniu obciążeń informacyjnych respondentów. W przypadku danych osobowych ich dalsze przetwarzanie do celów statystycznych jest, zgodnie z rozporządzeniem, operacją przetwarzania zgodną z prawem. Dodatkowo, dane pozyskane z tego źródła, tak samo jak dane pozyskiwane z innych źródeł, będą objęte tajemnicą statystyczną, która gwarantuje ich poufność i wykorzystanie wyłącznie w celu statystycznym.

W pkt 2 zmiana art. 4 ust. 2 wynika z wprowadzenia rozdziału 2a i konieczności doprecyzowania przepisu w zakresie spisów powszechnych.

W pkt 3 wprowadzone zostało nowe brzmienie art. 5 w celu jednoznacznego wskazania działań wykonywanych przez służby statystyki publicznej w związku z realizowaniem zadań określonych w ustawie. Podkreślona została zasada nieodpłatnego dostępu do danych, co koreluje z obowiązującym przepisem art. 13 ust. 1 oraz art. 53 ustawy. W związku z faktem, że zgodnie z art. 4 ust. 1 ustawy badania statystyczne statystyki publicznej mogą dotyczyć każdej dziedziny życia społecznego i gospodarczego oraz występujących w nim zjawisk konieczne jest zapewnienie dostępu do danych, niezbędnych do realizacji badań, a więc również tych objętych tajemnicami prawnie chronionymi, z wyłączeniem informacji

chronionych na podstawie przepisów o ochronie informacji niejawnych. Podkreślić należy, że wszystkie dane zbierane przez służby statystyki publicznej są objęte bezwzględną ochroną jaką gwarantuje tajemnica statystyczna i są wykorzystywane wyłącznie do prac statystycznych. Takie podejście wynika też bezpośrednio z art. 20 rozporządzenia rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylającego rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich (Dz. Urz. UE L 87 z 31.03.2009, str. 164, z późn. zm.), zwanym dalej „rozporządzeniem 223/2009".

W pkt 4 w dodawanym art. 5a wskazane zostały źródła danych wykorzystywanych przez służby statystyki publicznej. Art. 5a ust. 1 został przeniesiony z aktualnie obowiązującego art. 5 ust. 1 pkt 1. Ust. 2 odnosi się do źródeł danych wykorzystywanych dla potrzeb służb statystyki publicznej. W związku z rozwojem nowych technologii i możliwością wykorzystania nowych, publicznie dostępnych informacji i dbałością służb statystyki publicznej o zagwarantowanie podstaw działania w oparciu o przepisy ustawowe wprowadzone zostały ust. 3 i 4. Z kolei ust. 5 projektowanego art. 5a precyzuje format przekazywanych lub udostępnianych danych, odwołując się w tym zakresie do obowiązującego przepisu art. 18a ust. 2 i 3 ustawy o statystyce publicznej. Przepis ten określa aspekty techniczne przekazywania danych.

W pkt 5 wprowadzana jest zmiana w art. 6, i tak w ust. 1 doprecyzowane zostały metody zbierania danych od respondentów. Natomiast dodawane ust. 4 i 5 odnoszą się do zasad udziału w badaniach statystycznych osób fizycznych i osób fizycznych prowadzących działalność gospodarczą. W szczególności w przypadku badań, dotyczących działalności gospodarczej osób fizycznych konieczne było uszczegółowienie ogólnej zasady dobrowolnego udziału osób fizycznych w badaniach statystycznych prowadzonych przez służby statystyki publicznej. Ust. 5 został przeniesiony z obowiązującego art. 35b ust. 4.

W pkt 6 zmiana polegająca na uchyleniu w art. 7 ust. 2 związana jest ze zmianą brzmienia art. 5.

W pkt 7 zaproponowane zostało doprecyzowane brzmienie obecnego art. 8 ustawy, poprzez wprowadzenie nazewnictwa zgodnego z wdrażanym rozporządzeniem 2016/679 (art. 9 i 10). Co do zasady dane określane jako „dane sensytywne" mogą być zbierane wyłącznie na zasadzie dobrowolności udzielania odpowiedzi. Innymi słowy, zebranie tego rodzaju danych bezpośrednio od osoby, która udziela odpowiedzi będzie możliwe wyłącznie na podstawie jej świadomej i dobrowolnej decyzji.

W pkt 8 uchylenie art. 9 ust. 1 związane jest z wprowadzeniem nowego rozdziału dotyczącego ogólnych zasad prowadzenia spisów powszechnych. Natomiast zmiana w ust. 2 wynika z uchylenia ust. 1 tego przepisu.

W pkt 9, dotyczącym art. 10 ustawy o statystyce publicznej wprowadzono wyrazy „statystykę publiczną" w odniesieniu do zbierania danych, które objęte są tajemnicą statystyczną, tak aby jednoznacznie wskazać, że wszelkie dane zbierane przez służby statystyki publicznej są objęte tą tajemnica. Pozostała część konstrukcji przepisu nie uległa zmianie w stosunku do brzmienia obecnie obowiązującego.

W pkt 10, dotyczącym art. 13 ustawy o statystyce publicznej zmiany wynikają z wprowadzenia do przepisów ustawy konstrukcji niepublicznych systemów informacyjnych.

W pkt 11 zmiana dotyczy terminu przekazania przez Radę Statystyki programu badań statystycznych statystyki publicznej (PBSSP) Radzie Ministrów, która zgodnie z art. 18 ustawy ustala program badań statystycznych w drodze rozporządzenia. Termin ten jest skorelowany z terminem przekazania projektu ustawy budżetowej. Przepis będzie miał zastosowanie do programu badań statystycznych statystyki publicznej na rok 2019 i lata kolejne.

W pkt 12 wprowadzony został nowy rozdział 2b Spisy powszechne.

Wprowadzenie do ustawy o statystyce publicznej nowego rozdziału, dotyczącego spisów powszechnych ma na celu uspójnienie w ramach statystyki publicznej przepisów, dotyczących wszystkich realizowanych w ramach systemu statystycznego badań statystycznych. Wprowadzenie omawianej zmiany w ramach nowelizacji związanej z wejściem w życie przepisów rozporządzenia nr 2016/679 znajduje swoje uzasadnienie w tym, iż spisy powszechne nie są niczym innym, jak badaniem statystycznym, a tym samym, powinny w stosunku do nich obowiązywać takie same zasady przetwarzania i ochrony danych, jak w stosunku do innych badań statystycznych. Proponowana zmiana ustawy pozwoli na regulację zadań nałożonych na Prezesa GUS, zwłaszcza tych związanych

z wyłączeniem albo ograniczeniem obowiązków wynikających z zapisów rozporządzenia nr 2016/679. Pozwoli też na uniknięcie wątpliwości, czy wyłączenia i ograniczenia obowiązków wynikających z rozporządzenia dotyczą też badań statystycznych, jakimi są spisy powszechne.

W proponowanej zmianie przepisy dotyczące spisów powszechnych stanowią odrębny rozdział, w którym znajdą się kwestie związane z organizacją i prowadzeniem spisów powszechnych, z których najbliższe planowane są na rok 2020 i 2021, jak też dla wszystkich prowadzonych w przyszłości spisów. W rozdziale tym ujęte zostały przepisy dotyczące obowiązku przekazywania danych, etapów prac spisowych, przepisy dotyczące struktury aparatu spisowego, czy wreszcie przepisy dotyczące finansowania prac spisowych.

Przepisy dotyczące spisów powszechnych będą także umiejscowione w innych rozdziałach ustawy o statystyce, tam gdzie uregulowane są zasady ogólne dla wszystkich prowadzonych badań statystycznych.

W zakresie nieunormowanym w ustawie będą przygotowywane odrębne regulacje ustawowe, których materię stanowić będzie zakres podmiotowy i przedmiotowy spisów powszechnych. Docelowo regulacje te będą ograniczone do obowiązków nakładanych na osoby fizyczne i wówczas będą określały szczegółowy zakres danych przekazywanych przez te osoby.

W pkt 13, wprowadzającym zmiany w art. 25 ustawy uszczegółowione zostały przepisy dotyczące zadań Prezesa Głównego Urzędu Statystycznego, co ma na celu dostosowanie do aktualnych potrzeb i jest odpowiedzią na zachodzące zmiany w postrzeganiu roli organu. Natomiast w związku z przyjętą konstrukcją w obowiązującej ustawie o statystyce publicznej, zgodnie z którą zadania dyrektorów urzędów statystycznych są określane poprzez odesłanie do zadań Prezesa Głównego Urzędu Statystycznego doprecyzowania wymagał również ust. 2 art. 25.

W pkt 14, dotyczącym art. 25a ustawy zmiana wynika z wprowadzenia we wcześniejszym przepisie - projektowanym pkt 8e – skrótu rozporządzenia Parlamentu 223/2009.

W pkt 15, dotyczącym art. 28 ustawy wprowadzona zmiana jest związana z przeniesieniem dotychczasowych przepisów dotyczących rachmistrzów spisowych do nowego rozdziału 2a.

W pkt 16-23 wprowadzone zostały zmiany w rozdziale 4a Przetwarzanie danych osobowych dla celów statystycznych. Zmiany te związane są z wprowadzeniem przepisów dostosowujących do rozporządzenia 2016/679 oraz wynikami analizy ex post obowiązujących przepisów.

W projektowanym art. 35a ust. 1 określone zostały cele statystyczne, w realizacji których niezbędne jest przetwarzanie danych osobowych. Zaproponowane rozwiązanie wychodzi naprzeciw dyspozycji ustawodawcy unijnego, który w art. 5 ust. 1 lit. b jako jedną z zasad przetwarzania danych osobowych wskazuje zbieranie ich w konkretnych, wyraźnych i prawnie uzasadnionych celach. Art. 35 ust. 3 odnosi się do krajowego rejestru urzędowego podmiotów gospodarki narodowej, którego prowadzenie jest jednym z zadań Prezesa Głównego Urzędu Statystycznego, realizowanym w ramach odrębnego od statystyki publicznej systemu informacyjnego administracji publicznej – art. 41 ust. 2.

Dodawany nowy art. 35aa określa administratora danych osobowych przetwarzanych przez służby statystyki publicznej, zarówno do celów statystycznych, jak i prowadzenia krajowego rejestru urzędowego podmiotów gospodarki narodowej. Organem, który ustala cele i sposoby przetwarzania danych osobowych jest Prezes Głównego Urzędu Statystycznego.

Powyższe przepisy art. 35aa-35ac pozwalają na realizację zasady przejrzystości, przez zamieszczenie informacji o tożsamości administratora i celach przetwarzania danych osobowych. Rozstrzygają też ewentualne wątpliwości co do tego, że Prezes Głównego Urzędu Statystycznego jest organem decydującym o celach i środkach przetwarzania danych.

Wprowadzone w art. 35b zmiany wynikają z analizy obowiązującego art. 35b ustawy. Ze względu na konieczność prowadzenia badań statystycznych z obszaru statystyki społecznej i demografii konieczne okazało się uszczegółowienie katalogu danych osobowych, do których przetwarzania na mocy ustawy zobowiązane są służby statystyki publicznej. Jednocześnie katalog celów, w jakich przetwarzane są te dane, został uściślony w stosunku do aktualnie obowiązującego. W związku z tym, że badania statystyczne mogą dotyczyć każdej dziedziny życia społecznego oraz występujących w nim zjawisk, to przewidziana została sytuacja, w której przetwarzanie danych osobowych we wskazanych obszarach może powodować powstanie dodatkowo innych danych o osobach, które to dane pierwotnie charakteru danych osobowych nie posiadały. Zmiana w art. 35b ust. 3 polega na dodaniu niepublicznych systemów informacyjnych, jako potencjalnego źródła danych osobowych dla potrzeb służb

statystyki publicznej. W art. 35b ust. 4, który nakładał obowiązek informacyjnych na służby statystyki publicznej został uchylony w związku z przeniesieniem jego treści do art. 6 ust. 5.

Zmiany w art. 35c w stosunku do obecnego brzmienia tego przepisu polegają na wprowadzeniu Centralnej Bazy Danych Ksiąg Wieczystych prowadzonej przez Ministra Sprawiedliwości oraz rejestru stanu cywilnego prowadzonego w systemie centralnym przez ministra właściwego do spraw informatyzacji do katalogu źródeł danych oraz doprecyzowaniu obowiązujących przepisów w związku z wprowadzeniem niepublicznych systemów administracyjnych, jako potencjalnego źródła danych osobowych dla potrzeb realizacji celów statystycznych.

Art. 35d związany jest ze szczególnym charakterem badań statystycznych. Co do zasady opracowywanie danych statystycznych, a takimi danymi są również i dane osobowe zebrane w ramach statystyki publicznej – projektowany art. 35ac – odbywa się z odłączeniem lub zakodowaniem informacji pozwalających na identyfikację konkretnego podmiotu obserwacji statystycznej. Sposób i tryb pseudonimizacji danych osobowych na potrzeby realizacji zadań określonych w ustawie przez służby statystyki publicznej będzie określał dokument opracowany i wydany przez Prezesa Głównego Urzędu Statystycznego, w drodze zarządzenia. Pseudonimizacja jest jednym ze sposobów zabezpieczenia danych, do których zachęca rozporządzenie 2016/679 (art. 32 ust. 1 lit. a), zatem ustawowe zagwarantowanie pseudonimizacji stanowi wyjście naprzeciw oczekiwaniom prawodawcy unijnego. Projektowany ust. 2 związany jest ze specyfiką badań statystycznych, które wymagają, w uzasadnionych przypadkach, dla osiągnięcia celu badania łączenia danych statystycznych pochodzących z różnych źródeł. Działanie takie podyktowane jest również dążeniem do wtórnego wykorzystania danych zgromadzonych w różnego rodzaju rejestrach i systemach informacyjnych lub zebranych na potrzeby innych badan statystycznych, tak by stale zmniejszać poziom obciążeń respondentów i ograniczać obowiązki informacyjne obywateli i przedsiębiorców. Należy również podnieść, że ustawodawca unijny pozwala na dalsze przetwarzania i wskazuje, że takie działanie w myśl art. 89 ust. 1 rozporządzenia 2016/679 nie jest niezgodne z pierwotnymi celami, co znalazło odzwierciedlenie w art. 5 ust. 1 lit. b ww. rozporządzenia.

Zasady, dotyczące przetwarzania danych osobowych przez służby statystyki publicznej, stosowane są również przez inne organy i podmioty, które prowadzą badania statystyczne w ramach programu badań statystycznych statystyki publicznej. Projektowany art. 35g, który

reguluje te kwestie również na gruncie obowiązujących przepisów, został uszczegółowiony, tak aby odpowiadał zmianom wprowadzanym w rozdziale 4a.

Projektowany art. 35h jest nowym rozwiązaniem i w całości jest związany z rozporządzeniem 679/2012. Zgodnie z brzmieniem punktu 2 artykułu 89 rozporządzenia 2016/679 statystyka publiczna może zostać wyłączona z wypełniania obowiązków nałożonych art. 15, 16, 18, 21, gdy przepisy prawa unijnego lub prawa państwa członkowskiego przewidzą wyjątki od praw, o których w nich mowa w sytuacjach, gdy istnieje prawdopodobieństwo, że prawa te uniemożliwią lub utrudnią realizację celów statystycznych i jeżeli wyjątki te są konieczne do realizacji tych celów.

Należy podkreślić, że wykonanie art. 15 ww. rozporządzenia pociągałoby dodatkowe obciążenia finansowe i administracyjne dla statystyki publicznej. Skuteczne realizowanie prawa dostępu osoby fizycznej, której dane dotyczą w przypadku statystyki publicznej jest trudne do wykonania ze względu na prowadzone w jej ramach duże badania wykorzystujące dane zebrane z kilku źródeł administracyjnych lub badania obejmujące całe społeczeństwo (spisy powszechne). Statystyka publiczna z natury rzeczy prowadzi najszerzej zakrojone badania, dotyczące dużych części lub całości populacji. Możliwość skorzystania z prawa dostępu do danych może powodować ogromne koszty, a jednocześnie warto podkreślić, że w przeciwieństwie do sektora prywatnego źródła danych osobowych służb statystyki publicznej są uregulowane w przepisach prawa. Zatem, obywatele mają świadomość tego, jakie dane mogą być przetwarzane przez statystykę publiczną, ponieważ albo oni sami byli źródłem tych danych, albo dane pochodzą z rejestrów publicznych regulowanych ustawami, albo też z rejestrów niepublicznych, którym udostępnili dane w związku z korzystaniem z ich usług. Zakres danych w niektórych z tych rejestrów jest określony przepisami prawa, jak np. w Prawie telekomunikacyjnym. Przyjęty sposób postępowania, tzn. wskazanie Prezesa Głównego Urzędu Statystycznego w przepisach prawnych, jako podmiotu upoważnionego do wykorzystywania gromadzonych przez inne organy i podmioty danych powoduje, że powszechna jest wiedza, jakie dane mogą być wykorzystywane przez służby statystyki publicznej. Warto również przypomnieć, że sama ustawa o statystyce publicznej zawiera zamknięty katalog danych osobowych, które mogą być wykorzystywane przez służby statystyki publicznej.

Trzeba mieć również na uwadze fakt, że żądanie dostępu do danych, ich sprostowania lub sprzeciwu wobec ich przetwarzania (określone w art. 15, 16, 21 rozporządzenia) przez podmiot może nastąpić po opracowaniu danych statystycznych (spseudonimizowaniu

i zanonimizowaniu) oraz publikacji wynikowych informacji statystycznych, do których opracowania posłużyły. Tym samym dotarcie do danych konkretnego podmiotu będzie obiektywnie niemożliwe.

W przypadku prawa do ograniczania przetwarzania danych - art. 18 rozporządzenia, należy podnieść, że przedmiotowa nowelizacja umacnia podstawy prawne przetwarzania danych osobowych, zgodnie z wymogami stawianymi przez rozporządzenia. Ponadto spełnienie ww. obowiązków przez służby statystyki publicznej może okazać się niemożliwe lub wymagające niewspółmiernie dużego wysiłku. I tu również należy podkreślić skalę działania służb statystyki publicznej oraz związany z nią duży koszt realizacji wspomnianych praw jednostki.

Z uwagi na fakt, iż dane wykorzystywane są wyłącznie dla celów statystycznych, osoba fizyczna, której dane są przetwarzane nie ponosi żadnych szkód w przypadku zastosowania wyjątków od praw, zgodnie z przyznaną możliwością w art. 89 ust. 2 rozporządzenia, dla statystyki publicznej, nie spowoduje to również jakiegokolwiek uszczerbku dla ochrony danych osobowych tej osoby przetwarzanych przez statystykę publiczną, gdyż nie są one wykorzystywane w żadnym innym celu niż statystyczny, tj.: wyłącznie do opracowywania i tworzenia wyników oraz analiz statystycznych i nie ma jakiegokolwiek wpływu na sytuację jednostki. Dane osobowe są dostępne tylko i wyłącznie określonemu kręgowi osób, w związku z wykonywaniem przez nich zadań służbowych, po złożeniu pisemnego oświadczenia o przestrzeganiu zasad poufności przetwarzanych danych i ich ochrony. Ponadto w zakresie ograniczenia prawa wskazanego w art. 12 i art. 13 rozporządzenia 2016/679, dotyczącego przejrzystej i „wszelkiej" komunikacji z podmiotem danych oraz przekazania podstawowych informacji na temat procesów przetwarzania danych, należy zauważyć, że motyw 62 preambuły rozporządzenia 2016/679 wyraźnie wskazuje, iż ograniczenie obowiązków informacyjnych wobec podmiotów danych jest w szczególności możliwe wtedy, kiedy przetwarzanie danych ma miejsce na podstawie przepisów prawa, podmiot danych dysponuje informacjami dotyczącymi szczegółów operacji przetwarzania danych lub wykonanie obowiązku wobec podmiotów danych wymagałoby niewspółmiernie dużego wysiłku. W motywie tym podkreśla się, że „sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia." Z kolei motyw 63 stwierdza, że „każda osoba fizyczna

powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (…).”.

Mając na względzie wagę i potrzebę zapewnienia rozliczalności, określonej w art. 5 ust. 2 rozporządzenia, przestrzegania zasad Prezes Głównego Urzędu Statystycznego zapewnia wszelkie środki techniczne i organizacyjne pozwalające osiągnąć mu ten cel. Niemniej, z uwagi na ilość przetwarzanych danych w różnych działaniach zapewnienie pełnej rozliczalności może nie być w pełni fizycznie wykonalne.

W pkt 24 zmiana w art. 39 związana jest ze zmianami w rozdziale 4a.

W pkt 25 wprowadzony został nowy rozdział 5a Operat do badań statystycznych.

Operat do badań statystycznych (OBS) jest narzędziem umożliwiającym prowadzenie badań statystycznych, w tym spisów powszechnych. Ze względu na jego istotną rolę w pracach służb statystyki publicznej i przetwarzanie w nim danych osobowych, dotychczasowe przepisy ustawy o statystyce publicznej dotyczące operatu do badań statystycznych zostały przeniesione do nowego rozdziału i uszczegółowione.

Wychodząc naprzeciw oczekiwaniom Europejskiej Komisji Gospodarczej ONZ dotyczącym przechowywania zbiorów jednostkowych ze spisów, zaproponowany został zapis umożliwiający przetwarzanie w OBS danych osobowych przez okres maksymalnie 100 lat.

Podkreślić należy, że również ustawodawca unijny w art. 5 ust. 1 lit. e wskazał na możliwość dłuższego przechowywania danych, jeżeli są one przetwarzane do celów statystycznych, zgodnie z art. 89 ust. 1. Tak wskazany okres przechowywania danych z prowadzonych badań statystycznych znajduje swoje uzasadnienie w specyfice działalności służb statystyki publicznej. Uzasadnieniem tego jest konieczność dokonania odpowiednich porównań, czy zachowania ciągów czasowych. Zadaniem statystyki publicznej jest bowiem zapewnienie rzetelnej, obiektywnej i systematycznej informacji m.in. o sytuacji ekonomicznej, demograficznej, społecznej oraz środowiska naturalnego. Niezwykle istotny w przypadku gromadzonych i analizowanych danych jest także aspekt historyczny.

Projektowana zmiana zapewnia gwarancje ochrony przetwarzanych danych statystycznych przez odesłanie do bezwzględnej tajemnicy, jaką jest tajemnica statystyczna i wprowadza zapisy umożliwiające dostęp do gromadzonych danych jedynie na wniosek i tylko podmiotów współprowadzących badania statystyczne w ramach programu badań

statystycznych statystyki publicznej, co więcej ograniczając dostęp do danych adresowych i wprowadzając dodatkowy wymóg określania przez współprowadzących badania celu i zakresu udostępnianych danych oraz środków ochrony i zabezpieczenia przed nieuprawnionym dostępem.

W pkt 26 wprowadzony został w art. 41 ust. 1a, który wskazuje administratora danych osobowych przetwarzanych w krajowym rejestrze urzędowym podmiotów gospodarki narodowej REGON.

Zmiana określona w pkt 27 związana jest z przeniesieniem definicji osoby fizycznej prowadzącej działalność gospodarczą do art. 2 ustawy (projektowany pkt 11b).

W pkt 28 zmiana w art. 53 związana jest z wprowadzeniem do ustawy konstrukcji niepublicznego systemu informacyjnego.

24. Ustawa z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników

Propozycja dodania art. 15c dopuszcza, w sytuacji przetwarzania danych osobowych w CRP KEP, możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i art. 34 RODO. Ograniczenie praw podmiotów danych jest możliwe na podstawie art. 23 ust. 1 lit. d i e RODO, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym 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 oraz 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. W przypadku art. 15c ograniczenie to zostało zastosowane w zakresie niezbędnym do realizowania zadań ustawowych przez Szefa Krajowej Administracji Skarbowej przy pomocy CRP KEP.

Przepis zawiera ponadto o 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.

25. Zmiany w ustawie z dnia 21 listopada 1996 r. o muzeach

W projektowanych przepisach uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych, podmiot uprawniony do przetwarzania oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań ustawowych. Z tego względu zaproponowano zmiany określające obowiązek przetwarzania danych osobowych przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego oraz muzea.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister oraz muzeum jako podmioty publiczne narażeni byliby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony danych, na podstawie art. 34 rozporządzenia 2016/679, z jednoczesnym zobowiązaniem do umieszczenia na stronie podmiotowej w Biuletynie Informacji Publicznej komunikatu o naruszeniu ochrony w ciągu 72 godzin od stwierdzenia naruszenia.

Prawa określone w art. 13 i 14 rozporządzenia 2016/679 (prawo do informacji), a także art. 19 rozporządzenia 2016/679 (obowiązek poinformowania odbiorców o sprostowaniu danych) również byłyby ograniczone ze względu na wysoki koszt. Proponujemy także ograniczenie stosowania art. 5 ust. 2 rozporządzenia 2016/679 z uwagi na konieczność ponoszenia niewspółmiernych do skali zadań nakładów, nie tylko finansowych.

26. Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne

Proponowana zmiana wynika z konieczności doprecyzowania skutku wykreślenia danych z rejestru poprzez wyraźne określenie, że wykreślenie z danego rejestru jest równoznaczne z fizycznym usunięciem z tego rejestru danych wykreślanego podmiotu. Pozwoli to uniknąć wątpliwości pojawiających się w związku z obecnym brzmieniem przepisu czy dane podmiotu wykreślonego są nadal widoczne, ale np. z adnotacją „wykreślony" lub odpowiadającym jej oznaczeniem graficznym. Należy jednocześnie wskazać, że wszystkie wykreślane dane nadal znajdują się w złożonych do organu rejestrowego wnioskach o wpis do rejestru, które stanowią akta sprawy. Ponieważ organ rejestrowy – Prezes Urzędu Regulacji Energetyki jest organem państwowym, do postępowania z aktami sprawy stosuje przepisy ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2016 r. poz. 1506, z późn. zm.), w rozumieniu której, akta sprawy są materiałem archiwalnym podlegającym archiwizacji przez okres czasu zgodny z nadaną im kategorią, zgodnie z wewnętrzną instrukcją kancelaryjną. W związku z tym, zrezygnowano z wprowadzania do ustawy – Prawo energetyczne przepisu określającego okres przechowywania wniosków o wpis do rejestru.

27. Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym oraz ustawa z dnia 24 lipca 2015 r. o zmianie ustawy – Prawo o ruchy drogowym

W związku z wejściem w życie w dniu 25 maja 2018 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „rozporządzeniem 2016/679", zaistniała potrzeba uregulowania pewnych szczególnych kwestii na poziomie ustawodawstwa krajowego, w tym w ustawie Prawo o ruchu drogowym oraz w ustawie z dnia 24 lipca 2015 r. o zmianie ustawy Prawo o ruchu drogowym oraz niektórych innych ustaw w zakresie centralnej ewidencji pojazdów, centralnej ewidencji kierowców oraz centralnej ewidencji posiadaczy kart parkingowych.

I. Centralna ewidencja pojazdów.

1. Zgodnie z projektowanymi przepisami w art. 80a ustawy proponuje się dodanie w ust. 5 przepisu wskazującego zakres danych osobowych przetwarzanych przed administratora danych i informacji zgromadzonych na potrzeby centralnej ewidencji pojazdów. W szczególności, wskazuje się takie dane osobowe jak: imię i nazwisko, numer PESEL, a w przypadku osoby nieposiadającej numeru PESEL - serię, numer i nazwę dokumentu potwierdzającego tożsamość, datę i miejsce urodzenia, adres zamieszkania oraz identyfikator osoby dokonującej w ewidencji wprowadzenia lub zmiany danych. Dane te będą przetwarzane w zakresie niezbędnym dla realizacji zadań określonych w art. 80a.

2. W kolejnym ust. 5a, wskazuje się, że podmioty, o których mowa w art. 80ba ust. 1, tj. podmioty zobowiązane do przekazywania danych do ewidencji oraz w art. 80c ust. 1 i ust. 2a, tj. podmioty, którym dane z ewidencji są udostępniane, przetwarzają ww. dane osobowe, w zakresie w jakim jest to niezbędne dla realizacji ich ustawowych zadań, przy jednoczesnej konieczności wdrożenia odpowiednich środków technicznych i organizacyjnych w celu ochrony tych danych osobowych.

3. Administrator danych i informacji przetwarzający dane osobowe na potrzeby centralnej ewidencji pojazdów, na mocy art. 80b ust. 4 Prd został zwolniony z obowiązku informacyjnego, określonego w art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Konieczność dostosowania przepisów krajowych do rozporządzenia 2016/679, wymaga stworzenia w poszczególnych przepisach krajowych takich rozwiązań, które umożliwią stosowanie wyłączenia obowiązku informacyjnego określonego w art. 14 rozporządzenia 2016/679, z tym, że uwzględniającego jednocześnie ograniczenia przewidziane w art. 23 ust. 2 w przedmiocie stosowania tego wyłączenia.

W przypadku centralnej ewidencji pojazdów, wręcz koniecznym i niezbędnym pozostaje utrzymanie dotychczasowego „statusu quo", w zakresie zwolnienia z obowiązku informacyjnego określonego w art. 14 ust. 2 rozporządzenia 2016/679 - przewidzianego dla administratora tej ewidencji. To najszersze wyłączenie obowiązku informacyjnego, przy gromadzeniu danych z innych źródeł (aniżeli od osoby, której dane dotyczą), dotyczy przypadków, gdy dane są przetwarzane przez administratora będącego podmiotem publicznym. Zgodnie natomiast z pkt 45 preambuły do rozporządzenia 2016/679, jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo UE lub

prawo państwa członkowskiego. Takie rozwiązanie znajduje właśnie oparcie w art. 80a ust. 5b ustawy, które wyłącza z obowiązku informacyjnego ewidencję, w której figuruje ok. 33 mln pojazdów. Udzielenie takich informacji okazałoby się praktycznie niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku i nakładów, zwłaszcza, że dotyczy przypadków przetwarzania, m.in. do celów archiwalnych, w interesie publicznym lub do celów statystycznych.

4. W kolejnych przepisach przewiduje się wyłączenia ze stosowania innych przepisów rozporządzenia 2016/679, w celu realizacji zadań władzy publicznej oraz zapewnienia prawidłowego funkcjonowania organów realizujących zadania publiczne. Dane osobowe zgromadzone w centralnej ewidencji pojazdów podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu tych danych, które następnie zostaną opisane w stosownych politykach bezpieczeństwa danych osobowych.

W ramach przetwarzania danych osobowych na potrzeby prowadzenia centralnej ewidencji pojazdów, ze stosowania rozporządzenia 2016/679 wyłączono:

• art. 15 rozporządzenia 2016/679, gdyż biorąc pod uwagę masowy charakter przetwarzania danych, wprowadzenie wszystkich wymagań określonych art. 15 rozporządzenia 2016/679 wymagałaby niewspółmiernie dużego nakładu środków, aby uzyskać pełną zgodność przekazywanych danych z wymaganiami rozporządzenia. Niemniej jednak należy wskazać, że przepisy ustawy jasno wskazują zasady udzielania osobom informacji o przetwarzanych danych osobowych, zatem postulat dostępu osoby do informacji, o tym jakie jej dane osobowe są przetwarzane pozostaje spełniony;

• art. 18 rozporządzenia 2016/679, z uwagi na konieczność zapewnienia istnienia możliwości nieprzerwanego przetwarzania danych przez organy publiczne, zatem ograniczenie przetwarzania danych jest niedopuszczalne;

• art. 19 rozporządzenia 2016/679, gdyż biorąc pod uwagę masowy charakter przetwarzania danych, wprowadzenie wszystkich wymagań określonych art. 19 rozporządzenia 2016/679 wymagałaby niewspółmiernie dużego nakładu środków lub też okazałoby się to praktycznie niemożliwe z przyczyn obiektywnych;

• art. 20 rozporządzenia 2016/679, gdyż prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

• art. 21 rozporządzenia 2016/679, albowiem przetwarzane w ewidencji dane są kluczowe dla bezpieczeństwa ruchu drogowego, zatem nie jest dopuszczalne zaprzestanie przetwarzania danych danej osoby na podstawie jej sprzeciwu.

5. Zgodnie z projektowanym ust. 6 w art. 80a, utrzymanie i rozwój centralnej ewidencji pojazdów zapewnia minister właściwy do spraw informatyzacji. W tym celu podejmuje on działania mające na celu: zapewnienie ochrony przed nieuprawnionym dostępem do ewidencji, zapewnienie integralności danych w ewidencji, zapewnienie dostępności systemu teleinformatycznego, w którym ewidencja jest prowadzona dla podmiotów przetwarzających dane i informacje, określenie zasad bezpieczeństwa przetwarzanych danych i informacji, w tym danych osobowych oraz zapewnienie rozliczalności ewidencji.

II. Centralna ewidencja kierowców.

1. Zgodnie z projektowanymi przepisami w art. 100a ustawy proponuje się dodanie w ust. 6 przepisu wskazującego zakres danych osobowych przetwarzanych przed administratora danych i informacji zgromadzonych na potrzeby centralnej ewidencji kierowców. W szczególności, wskazuje się takie dane osobowe jak: imię i nazwisko, numer PESEL, a w przypadku osoby nieposiadającej numeru PESEL - serię, numer i nazwę dokumentu potwierdzającego tożsamość, data i miejsce urodzenia, adres zamieszkania, unikalny numer identyfikujący profil kandydata na kierowcę, identyfikator osoby dokonującej w ewidencji zamieszczenia lub zmiany danych, fotografię, wzór podpisu, numer telefonu oraz adres poczty elektronicznej. Dane te będą przetwarzane w zakresie niezbędnym dla realizacji zadań określonych w art. 100a.

2. W kolejnym ust. 6a, wskazuje się, że podmioty, o których mowa w art. 100b ust. 2, tj. podmioty zobowiązane do przekazywania danych do ewidencji oraz w art. 100c ust. 1 i ust. 1a, tj. podmioty, którym dane z ewidencji są udostępniane, przetwarzają ww. dane osobowe, w zakresie w jakim jest to niezbędne dla realizacji ich ustawowych zadań, przy jednoczesnej konieczności wdrożenia odpowiednich środków technicznych i organizacyjnych w celu ochrony tych danych osobowych.

3. Administrator danych i informacji przetwarzający dane osobowe na potrzeby centralnej ewidencji kierowców, na mocy art. 100b ust. 4 Prd został zwolniony z obowiązku informacyjnego określonego w art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Konieczność dostosowania przepisów krajowych do rozporządzenia 2016/679, wymaga stworzenia w poszczególnych przepisach krajowych takich rozwiązań,

które umożliwią stosowanie wyłączenia obowiązku informacyjnego określonego w art. 14 rozporządzenia 2016/679, z tym, że uwzględniającego jednocześnie ograniczenia przewidziane w art. 23 ust. 2 w przedmiocie stosowania tego wyłączenia.

W przypadku centralnej ewidencji kierowców, wręcz koniecznym i niezbędnym pozostaje utrzymanie dotychczasowego „statusu quo", w zakresie zwolnienia z obowiązku informacyjnego określonego w art. 14 ust. 2 rozporządzenia 2016/679 - przewidzianego dla administratora tej ewidencji. To najszersze wyłączenie obowiązku informacyjnego, przy gromadzeniu danych z innych źródeł (aniżeli od osoby, której dane dotyczą), dotyczy przypadków, gdy dane są przetwarzane przez administratora będącego podmiotem publicznym. Zgodnie natomiast z pkt 45 preambuły do rozporządzenia 2016/679, jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Takie rozwiązanie znajduje właśnie oparcie w art. 100a ust. 5b ustawy, które wyłącza z obowiązku informacyjnego ewidencję, w której figuruje ok. 21 mln osób. Udzielenie takich informacji okazałoby się praktycznie niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku i nakładów, zwłaszcza, że dotyczy przypadków przetwarzania, m.in. do celów archiwalnych, w interesie publicznym lub do celów statystycznych.

4. W kolejnych przepisach przewiduje się wyłączenia ze stosowania innych przepisów rozporządzenia 2016/679, w celu realizacji zadań władzy publicznej oraz zapewnienia prawidłowego funkcjonowania organów realizujących zadania publiczne. Dane osobowe zgromadzone w centralnej ewidencji kierowców podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu tych danych, które następnie zostaną opisane w stosownych politykach bezpieczeństwa danych osobowych.

W ramach przetwarzania danych osobowych na potrzeby prowadzenia centralnej ewidencji kierowców, ze stosowania rozporządzenia 2016/679 wyłączono:

• art. 15 rozporządzenia 2016/679, gdyż biorąc pod uwagę masowy charakter przetwarzania danych, wprowadzenie wszystkich wymagań określonych art. 15 rozporządzenia 2016/679 wymagałaby niewspółmiernie dużego nakładu środków, aby uzyskać pełną zgodność przekazywanych danych z wymaganiami rozporządzenia. Niemniej jednak należy wskazać, że

przepisy ustawy jasno wskazują zasady udzielania osobom informacji o przetwarzanych danych osobowych, zatem postulat dostępu osoby do informacji, o tym jakie jej dane osobowe są przetwarzane pozostaje spełniony;

• art. 18 rozporządzenia 2016/679, z uwagi na konieczność zapewnienia istnienia możliwości nieprzerwanego przetwarzania danych przez organy publiczne, zatem ograniczenie przetwarzania danych jest niedopuszczalne;

• art. 19 rozporządzenia 2016/679, gdyż biorąc pod uwagę masowy charakter przetwarzania danych, wprowadzenie wszystkich wymagań określonych art. 19 rozporządzenia 2016/679 wymagałaby niewspółmiernie dużego nakładu środków lub też okazałoby się to praktycznie niemożliwe z przyczyn obiektywnych;

• art. 20 rozporządzenia 2016/679, gdyż prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

• art. 21 rozporządzenia 2016/679, albowiem przetwarzane w ewidencji dane są kluczowe dla bezpieczeństwa ruchu drogowego, zatem nie jest dopuszczalne zaprzestanie przetwarzania danych danej osoby na podstawie jej sprzeciwu.

5. Zgodnie z projektowanym ust. 7 w art. 100a, utrzymanie i rozwój centralnej ewidencji kierowców zapewnia minister właściwy do spraw informatyzacji. W tym celu podejmuje on działania mające na celu: zapewnienie ochrony przed nieuprawnionym dostępem do ewidencji, zapewnienie integralności danych w ewidencji, zapewnienie dostępności systemu teleinformatycznego, w którym ewidencja jest prowadzona dla podmiotów przetwarzających dane i informacje, określenie zasad bezpieczeństwa przetwarzanych danych i informacji, w tym danych osobowych oraz zapewnienie rozliczalności ewidencji.

III. Centralna ewidencja posiadaczy kart parkingowych.

1.Zgodnie z projektowanymi przepisami w art. 100f ustawy proponuje się dodanie w ust. 4 przepisu wskazującego zakres danych osobowych przetwarzanych przed administratora danych i informacji zgromadzonych na potrzeby centralnej ewidencji posiadaczy kart parkingowych. W szczególności, wskazuje się takie dane osobowe jak: imię i nazwisko, numer PESEL, a w przypadku osoby nieposiadającej numeru PESEL - serię, numer i nazwę dokumentu potwierdzającego tożsamość, identyfikator osoby dokonującej w ewidencji wprowadzenia lub

zmiany danych oraz numer karty wydanej dla osoby. Dane te będą przetwarzane w zakresie niezbędnym dla realizacji zadań określonych w art. 100f.

2. W kolejnym ust. 4a, wskazuje się, że podmioty, o których mowa w art. 100g ust. 2, tj. powiatowe zespoły do spraw orzekania o niepełnosprawności, jako podmioty zobowiązane do przekazywania danych do ewidencji oraz w art. 100k ust. 1, tj. podmioty, którym dane z ewidencji są udostępniane, przetwarzają ww. dane osobowe, w zakresie w jakim jest to niezbędne dla realizacji ich ustawowych zadań, przy jednoczesnej konieczności wdrożenia odpowiednich środków technicznych i organizacyjnych w celu ochrony tych danych osobowych.

3. Administrator danych i informacji przetwarzający dane osobowe na potrzeby centralnej ewidencji posiadaczy kart parkingowych, na mocy art. 100g ust. 7 ustawy z dnia 25 lipca 2015 r. o zmianie ustawy Prawo o ruchu drogowym oraz niektórych innych ustaw (Dz. U. z 2015 r. poz. 1273), został zwolniony z obowiązku informacyjnego określonego w art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Konieczność dostosowania przepisów krajowych do rozporządzenia 2016/679, wymaga stworzenia w poszczególnych przepisach krajowych takich rozwiązań, które umożliwią stosowanie wyłączenia obowiązku informacyjnego określonego w art. 14 rozporządzenia 2016/679, z tym, że uwzględniającego jednocześnie ograniczenia przewidziane w art. 23 ust. 2 w przedmiocie stosowania tego wyłączenia.

W przypadku centralnej ewidencji posiadaczy kart parkingowych, wręcz koniecznym i niezbędnym pozostaje utrzymanie dotychczasowych założeń w zakresie zwolnienia z obowiązku informacyjnego określonego w art. 14 ust. 2 rozporządzenia 2016/679 - przewidzianego dla administratora tej ewidencji. To najszersze wyłączenie obowiązku informacyjnego, przy gromadzeniu danych z innych źródeł (aniżeli od osoby, której dane dotyczą), dotyczy przypadków, gdy dane są przetwarzane przez administratora będącego podmiotem publicznym. Zgodnie natomiast z pkt 45 preambuły do rozporządzenia 2016/679, jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo UE lub prawo państwa członkowskiego. Takie rozwiązanie znajduje właśnie oparcie w art. 100f ust. 4 ustawy, które wyłącza z obowiązku informacyjnego ewidencję dotyczącą ok. 400 tyś. posiadaczy kart parkingowych. Udzielenie takich informacji okazałoby

się praktycznie niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku i nakładów, zwłaszcza, że dotyczy przypadków przetwarzania, m.in. do celów archiwalnych, w interesie publicznym lub do celów statystycznych.

4. W kolejnych przepisach przewiduje się wyłączenia ze stosowania innych przepisów rozporządzenia 2016/679, w celu realizacji zadań władzy publicznej oraz zapewnienia prawidłowego funkcjonowania organów realizujących zadania publiczne. Dane osobowe zgromadzone w centralnej ewidencji posiadaczy kart parkingowych podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu tych danych, które następnie zostaną opisane w stosownych politykach bezpieczeństwa danych osobowych.

W ramach przetwarzania danych osobowych na potrzeby prowadzenia centralnej ewidencji posiadaczy kart parkingowych, ze stosowania rozporządzenia 2016/679 wyłączono:

• art. 15 rozporządzenia 2016/679, gdyż biorąc pod uwagę masowy charakter przetwarzania danych, wprowadzenie wszystkich wymagań określonych art. 15 rozporządzenia 2016/679 wymagałaby niewspółmiernie dużego nakładu środków, aby uzyskać pełną zgodność przekazywanych danych z wymaganiami rozporządzenia. Niemniej jednak należy wskazać, że przepisy ustawy jasno wskazują zasady udzielania osobom informacji o przetwarzanych danych osobowych, zatem postulat dostępu osoby do informacji, o tym jakie jej dane osobowe są przetwarzane pozostaje spełniony;

• art. 18 rozporządzenia 2016/679, z uwagi na konieczność zapewnienia istnienia możliwości nieprzerwanego przetwarzania danych przez organy publiczne, zatem ograniczenie przetwarzania danych jest niedopuszczalne;

• art. 19 rozporządzenia 2016/679, gdyż biorąc pod uwagę masowy charakter przetwarzania danych, wprowadzenie wszystkich wymagań określonych art. 19 rozporządzenia 2016/679 wymagałaby niewspółmiernie dużego nakładu środków lub też okazałoby się to praktycznie niemożliwe z przyczyn obiektywnych;

• art. 20 rozporządzenia 2016/679, gdyż prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

• art. 21 rozporządzenia 2016/679, albowiem przetwarzane w ewidencji dane są kluczowe dla bezpieczeństwa ruchu drogowego, zatem nie jest dopuszczalne zaprzestanie przetwarzania danych danej osoby na podstawie jej sprzeciwu.

5. Zgodnie z projektowanym ust. 5 w art. 100f, utrzymanie i rozwój centralnej ewidencji posiadaczy kart parkingowych zapewnia minister właściwy do spraw informatyzacji. W tym celu podejmuje on działania mające na celu: zapewnienie ochrony przed nieuprawnionym dostępem do ewidencji, zapewnienie integralności danych w ewidencji, zapewnienie dostępności systemu teleinformatycznego, w którym ewidencja jest prowadzona dla podmiotów przetwarzających dane i informacje, określenie zasad bezpieczeństwa przetwarzanych danych i informacji, w tym danych osobowych oraz zapewnienie rozliczalności ewidencji.

28. Ustawa z dnia 27 czerwca 1997 r. o bibliotekach

W proponowanej zmianie przepisów 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) uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, zgodnie z którym przepis prawa krajowego powinien określać obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych, oraz rodzaj danych przetwarzanych w ramach poszczególnych zadań ustawowych.

W związku z powyższym w projekcie zaproponowano zmiany polegające na określeniu zakresu danych, których przetwarzanie jest konieczne w związku z wykonywaniem poszczególnych obowiązków ustawowych. Proponuje się także, aby administrator danych osobowych mógł pełnić funkcję podmiotu przetwarzającego dane osobowe lub zlecać przetwarzanie w swoim imieniu danych osobowych podmiotowi przetwarzającemu. Wprowadzono także możliwość zlecenia innym podmiotom przez administratora danych osobowych przetwarzania danych na swoją rzecz oraz pełnienia administratora danych osobowych funkcji przetwarzającego dane na zlecenie innego podmiotu.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i art. 15 rozporządzenia 2016/679 w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: administrator danych osobowych, w tym biblioteki, jako podmioty publiczne narażeni byliby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony danych, na podstawie art. 34 rozporządzenia 2016/679, wprowadzając zarazem normę nakazującą umieścić na stronie podmiotowej Biuletynu Informacji Publicznej informację o zaistniałym naruszeniu w terminie 72 godzin od stwierdzenia naruszenia. Nadmierne nakłady środków powodowałaby również konieczność dokumentowania czynności z zakresu ochrony danych, o której mowa w art. 5 ust. 2 rozporządzenia 2016/679, dlatego proponuje się ograniczenie tego obowiązku w stosunku do administratora danych osobowych.

Należy podkreślić, że administrator danych osobowych byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach przez umieszczenie stosownej informacji na stronie Biuletynu Informacji Publicznej.

29. Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami

Zmiana o charakterze porządkowym. W związku z tym, że Generalny Inspektor Ochrony Danych Osobowych w wyniku zmian wprowadzonych ustawą o ochronie danych osobowych stanie się Prezesem Urzędu Ochrony Danych Osobowych, a Biuro Generalnego Inspektora Ochrony Danych Osobowych przekształcone zostanie w Urząd Ochrony Danych Osobowych, konieczne stało się zastąpienie w ustawie wyrazów „Generalny Inspektor Ochrony Danych Osobowych” wyrazami „Prezes Urzędu Ochrony Danych Osobowych”.

30. Ustawa z dnia 27 lipca 2001 r. – Prawo o ustroju sadów powszechnych, ustawa z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych, ustawa z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych, w ustawie z dnia 23 listopada 2002 r. o Sądzie Najwyższym

Zgodnie z art. 1 § 2 i 3 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2016 r. poz. 2062, z późn. zm.) sądy powszechne sprawują wymiar sprawiedliwości oraz wykonują inne zadania z zakresu ochrony prawnej powierzone w drodze ustaw. W ramach realizacji swoich zadań sądy przetwarzają dane osób fizycznych. Jest to bowiem niezbędne dla zapewnienia należytego biegu toczącym się postępowaniom (doręczanie zawiadomień o rozprawach, informacji, pism i orzeczeń sądowych).

W wymiarze sprawiedliwości przetwarzanie danych osobowych ma miejsce zarówno w systemach teleinformatycznych obsługujących postępowania sądowe (np. elektroniczne postępowanie upominawcze), systemach teleinformatycznych, w których prowadzone są rejestry sądowe (np. elektroniczna księga wieczysta, Krajowy Rejestr Sądowy) oraz w sądowych systemach informatycznych (biurowość sądowa), jak również w postępowaniach sądowych prowadzonych w tradycyjny sposób.

Sposób przetwarzania danych osobowych (elektronicznie albo papierowo) determinuje administratora danych. Sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej są administratorem danych osobowych przetwarzanych w prowadzonych papierowo aktach spraw, a także w elektronicznych postępowaniach sądowych oraz rejestrach sądowych.

W odniesieniu do niektórych z funkcjonujących w sądach systemów teleinformatycznych administratorem danych osobowych jest również Minister Sprawiedliwości jako podmiot odpowiedzialny za utrzymanie systemu i zapewnienie jego bezpieczeństwa, a także jako zwierzchnik komórki organizacyjnej Ministerstwa Sprawiedliwości wykonującej w systemie czynności określone w przepisach szczególnych (np. udzielanie informacji z rejestrów sądowych, zakładanie konta w systemie teleinformatycznym obsługującym postępowanie sądowe).

W odniesieniu do sądowych systemów informatycznych, które wspierają pracę sądów, za administratora danych osobowych oprócz sądów należy również uznać prezesa właściwego sądu. Przepis § 82 zarządzenia Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej (Dz. Urz. MIN. Sprawiedl. poz. 22) upoważnia bowiem prezesa sądu do zarządzenia prowadzenia urządzeń ewidencyjnych przez sekretariaty sądów przy wykorzystaniu systemów informatycznych, zastępujących tradycyjne urządzenia ewidencyjne.

Mając powyższe na względzie w projektowanym art. 175d ustawy – Prawo o ustroju sądów powszechnych jako administratorów danych osobowych w systemach teleinformatycznych obsługujących postępowania sądowe, w systemach teleinformatycznych, w których prowadzone są rejestry sądowe oraz w sądowych systemach informatycznych wskazano: sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej, prezesów właściwych sądów oraz Ministra Sprawiedliwości w ramach realizowanych zadań.

Odrębnie natomiast określono administratorów danych osobowych w postępowaniach sądowych prowadzonych poza systemami teleinformatycznymi. Administratorami takich danych są wyłącznie sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej (projektowany art. 175e ustawy – Prawo o ustroju sądów powszechnych).

Mając na względzie, że stosownie do art. 178 ust. 1 ustawy z dnia 2 kwietnia 1997 r. Konstytucja Rzeczpospolitej Polskiej sędziowie w sprawowaniu swojego urzędu są niezawiśli i podlegają tylko konstytucji i ustawom, a przetwarzanie danych osobowych w postępowaniach sądowych oraz w rejestrach sądowych określają przepisy ustaw szczególnych regulujących poszczególne procedury sądowe oraz rejestry sądowe, za celowe i uzasadnione uznano wyłączenie stosowania niektórych przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Wprowadzenie takiego wyłączenia dopuszcza bowiem art. 23 ust. 1 pkt f rozporządzenia 2016/679.

Dane osobowe są przetwarzane w postępowaniach sądowych oraz rejestrach sądowych w celu wypełnienia obowiązku prawnego. Operacje i procedury, a także cel i podstawę prawną przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości w szerokim tego słowa znaczeniu, w sposób jasny i przejrzysty określają akty prawne regulujące poszczególne rodzaje postępowań sądowych oraz rejestrów sądowych. Przepisy poszczególnych procedur sądowych regulują również prawa osób, których dane dotyczą. Zważywszy na powyższe, a nadto na istniejące już duże obciążenie sądów czynnościami niezwiązanymi bezpośrednio ze sprawowaniem wymiaru sprawiedliwości, uzasadnione jest wyłączenie obowiązków informacyjnych z art. 13 i 14 rozporządzenia 2016/679. W przeciwnym razie można się spodziewać spadku wydajności sądów,

spowodowanego realizacją dodatkowych obowiązków, co oczywiście negatywnie odbije się na sprawności postępowań sądowych, w tym szeroko rozumianych postępowań rejestrowych.

Ze względu na określone w poszczególnych procedurach sądowych zasady dostępu do akt spraw i rejestrów sądowych celowe jest wyłączenie art. 15 rozporządzenia 2016/679. Jeżeli bowiem dane osobowe znajdują się w aktach spraw albo w rejestrach sądowych, to dostęp do tych danych może odbywać się tylko na zasadach określonych w przepisach ustaw szczególnych regulujących dostęp do akt spraw i rejestrów sądowych. Z kolei dostęp do sądowych systemów informatycznych, w których prowadzone są urządzenia ewidencyjne sądów mają tylko upoważnione osoby.

Wyłączenie art. 16 rozporządzenia 2016/679 jest konsekwencją zasady integralności akt, sprzeciwiającej się usuwaniu z akt tego, co zostało do nich złożone oraz dokonywaniu zmian w treści akt. Sprostowania w postępowaniach sądowych oraz rejestrach sądowych mogą odbywać się wyłącznie na zasadach określonych w konkretnych ustawach, regulujących procedury sądowe albo rejestry sądowe (np. art. 350 i 62613 § 2 Kodeksu postępowania cywilnego, art. 12 ust. 2 ustawy o Krajowym Rejestrze Sądowym). Przepisy tych ustaw regulują również odrębnie obowiązek powiadomienia o dokonanych przez sąd czynnościach, co uzasadnia wyłączenie także art. 19 rozporządzenia 2016/679.

Z wyżej przytoczonych powodów wyłączenia wymaga również art. 18 rozporządzenia 2016/679, jeżeli dane osobowe są gromadzone w postępowaniach sądowych, rejestrach sądowych oraz sądowych systemach informatycznych.

Zbyt duże obciążenie sądów czynnościami niezwiązanymi bezpośrednio ze sprawowaniem wymiaru sprawiedliwości uzasadnia wyłączenie art. 20 rozporządzenia 2016/679. Trzeba też mieć na względzie, że przetwarzanie danych osobowych w wymiarze sprawiedliwości jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator. Brak jest zatem uzasadnienia dla nałożenia na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania.

Proponuje się również wyłączenie art. 21 rozporządzenia 2016/679 z uwagi na odrębne w wymiarze sprawiedliwości zasady przetwarzania danych osobowych przez sądy. Należy stanowczo podkreślić, że z uwagi na to, że przetwarzanie danych osobowych w postępowaniach sądowych związane jest ze sprawowaniem wymiaru sprawiedliwości, zgromadzone w tych postępowaniach dane muszą być przechowywane tak długo, jak długo,

zgodnie z właściwymi przepisami, przechowywane są akt spraw sądowych oraz urządzenia ewidencyjne.

Przepisy regulujące rejestry sądowe, mając na względzie cel prowadzenia rejestrów, wyłączają z kolei trwałe usuwanie danych z systemów teleinformatycznych.

Reasumując, zważywszy, że obowiązujące przepisy regulujące postępowania sądowe oraz rejestry sądowe zapewniają wysoki i spójny stopień ochrony osób fizycznych.

Kolejne zaproponowane zmiany w art. 157g i 171a ustawy – Prawo o ustroju sądów powszechnych mają na celu spójne uregulowanie kwestii przetwarzania danych osobowych dotyczące stałych mediatorów, ławników i lekarzy sądowych. Przedstawione propozycje zostały oparte o uregulowanie odnoszące się do analogicznych kwestii jak w przypadku biegłych sądowych.

Zakres danych osobowych w przypadku stałych mediatorów oraz ławników określony został w postaci listy stałych mediatorów oraz listy ławników. Szczegółowy sposób prowadzenia listy stałych mediatorów został określony w odpowiednim akcie wykonawczym. W przypadku ławników zakres danych w postaci listy ławników przekazują właściwe rady gmin, po dokonaniu wyborów ławników.

W projektowanym art. 175f ustawy – Prawo o ustroju sądów powszechnych proponuje się wyłączenie przepisów art. 13-16 oraz 18-21 ogólnego rozporządzenia o ochronie danych.

Jednocześnie wskazać należy, że spełnione są przesłanki, o których mowa w art. 23 ust. 2 ogólnego rozporządzenia o ochronie danych. Właściwe akty prawne regulujące organizację sądów powszechnych, poszczególne procedury sądowe oraz rejestry sądowe określają podstawy prawne przetwarzania danych, cel przetwarzania danych, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty którym można ujawnić dane osobowe, administratorów danych, okres przechowywania, zabezpieczenia zapobiegające nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, a także ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

Zaproponowane w projektowanym art. 175f ustawy – Prawo o ustroju sądów powszechnych wyłączenie dotyczy przetwarzania danych we wszystkich postępowaniach sądowych prowadzonych w tradycyjny sposób jak i elektronicznie, obejmuje wszystkie ich etapy i podejmowane w nich czynności nie tylko przez sądy, ale również przez te podmioty,

które w postępowaniu sądowym wykonują czynności na zlecenie sądu np. biegli sądowi czy tłumacze przysięgli.

Należy przyjąć, że zaproponowane w projektowanym art. 175f ustawy – Prawo o ustroju sądów powszechnych wyłączenie obejmuje również udzielanie informacji z prowadzonych w systemach teleinformatycznych rejestrów sądowych przez utworzone w tym celu komórki organizacyjne Ministerstwa Sprawiedliwości. Wyłączenie to uzasadnia zakres zadań wyznaczonych tym komórkom w ustawach szczególnych. Żadna z centralnych informacji nie jest uprawniona do podejmowania czynności ingerujących w treść danych zamieszczanych w rejestrach. Rejestry prowadzą sądy i co do zasady to one są wyłącznie uprawnione do dokonywania wpisów w rejestrach. Rolą centralnych informacji jest wyłącznie udzielanie informacji o treści danych zamieszonych w rejestrach przez sądy.

Zaproponowane zmiany art. 157 i 175a ustawy – Prawo o ustroju sądów powszechnych uwzględniają odrębny charakter i przeznaczenie przetwarzania danych osobowych biegłych sądowych oraz osób ubiegających się o ustanowienie biegłymi sądowymi związane z prowadzonymi w odniesieniu do nich postępowaniami administracyjnymi i innymi czynnościami podejmowanymi wobec nich przez prezesów sądów okręgowych oraz Ministra Sprawiedliwości. W tym zakresie konieczne jest zapewnienie możliwości szybkiego podejmowania wobec nich zróżnicowanych czynności administracyjnych wynikających z wykonywanych przez te organy zadań, co związane jest z pozyskiwaniem i przekazywaniem danych osobowych. Czynności te mają charakter pomocniczy wobec czynności z zakresu wymiaru sprawiedliwości wykonywanych przez sądy. Ponieważ dotyczą ich jedynie pośrednio, za celowe uznać należy odrębne ich uregulowanie w proponowany sposób.

W ustawie – Prawo o ustroju sądów wojskowych, ustawie – Prawo o ustroju sądów administracyjnych oraz w ustawie o Sądzie Najwyższym zaproponowano rozwiązania analogiczne jak w ustawie – Prawo o ustroju sądów powszechnych. Sądy wojskowe, sądy administracyjne oraz Sąd Najwyższy podobnie jak sądy powszechne sprawują bowiem wymiar sprawiedliwości w ramach, którego przetwarzają dane osobowe. Dane przetwarza się w celu realizacji obowiązku prawnego. Konieczne jest zatem zachowanie odrębności postępowania z danymi osobowymi stosownie do reguł rządzących postępowaniami przed sądami administracyjnymi i Sądem Najwyższym.

Ze względu na specyfikę funkcjonowania sądownictwa w projekcie ustawy należało zawrzeć szczególną regulację dotyczącą nadzoru nad przetwarzaniem danych osobowych przez sądy. Art. 55 ust. 3 rozporządzenia 2016/679 wprowadza istotny wyłom od ogólnej zasady dotyczącej nadzoru nad przetwarzaniem danych osobowych. Jasno wskazuje się w nim, że organy nadzorcze (centralny organ nadzorczy państwa członkowskiego) nie są właściwe do nadzorowania operacji przetwarzania dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości. Jednakże motyw 20 tego rozporządzenia dopuszcza możliwość powierzenia nadzoru nad operacjami przetwarzania danych osobowych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego. Organy te, zgodnie z treścią motywu 20 ogólnego rozporządzenia o ochronie danych, powinny w szczególności zapewnić przestrzeganie przepisów ogólnego rozporządzenia, zwiększać wiedzę w wymiarze sprawiedliwości o jego obowiązkach wynikających z tego rozporządzenia oraz rozpatrywać skargi związane z operacjami przetwarzania danych.

W polskim systemie prawnym przetwarzanie danych osobowych w ramach sprawowania wymiaru sprawiedliwości dokonuje się w toku postępowań prowadzonych przez sądy powszechne, sądy wojskowe, sądy administracyjne (Naczelny Sąd Administracyjny i wojewódzkie sądy administracyjne), Sąd Najwyższy oraz Trybunał Konstytucyjny. W związku z tym proponuje się, aby nadzór nad przetwarzaniem danych osobowych dokonywany był w ramach prowadzonych przez te sądy postępowań sądowych. W pozostałym zakresie działalności sądów – innym niż dotyczący postępowań sądowych – nadzór pozostałby w zakresie właściwości centralnego organu nadzorczego.

Generalna zasada nadzoru oparta jest o system kontroli rozproszonej. Oznacza to, że nie wskazuje się jednego organu, który pełniłby funkcję organu nadzorczego, a jedynie istniejącym podmiotom powierza się pełnienie tej funkcji.

Planuje się, aby przetwarzanie danych osobowych przez sądy powszechne dokonywane w ramach prowadzonych postępowań sądowych podlegało nadzorowi:

- w zakresie działalności sądu rejonowego – prezesowi sądu okręgowego,

- w zakresie działalności sądu okręgowego – prezesowi sądu apelacyjnego,

- w zakresie działalności sądu apelacyjnego – Krajowej Radzie Sądownictwa.

Następnie, organem właściwym w zakresie nadzoru nad przetwarzaniem danych osobowych przez wojewódzkie sądy administracyjne będzie Prezes Naczelnego Sądu Administracyjnego, a w zakresie nadzoru nad przetwarzaniem danych osobowych przez Naczelny Sąd Administracyjny – Krajowa Rada Sądownictwa. W końcu, organem właściwym w zakresie nadzoru nad przetwarzaniem danych osobowych przez Sąd Najwyższy oraz Trybunał Konstytucyjny będzie wyłącznie Krajowa Rada Sądownictwa. Wymaga to także zmiany w ustawie o Krajowej Radzie Sądownictwa, wskazującej dodatkową kompetencję Rady.

Należy zauważyć, że podmioty będące organami nadzoru nad poszczególnymi sądami chociaż same pozostają w strukturze wymiaru sprawiedliwości, to zachowują samodzielność i niezależność od sądów podlegających nadzorowi.

Przewiduje się, że nadzór polegać będzie na ocenie przestrzegania przepisów rozporządzenia2016/679. Zakres zadań i uprawnień organów sprawujących nadzór nad przetwarzaniem danych osobowych w postępowaniach prowadzonych przez sądy został określony w oparciu o zadania i uprawnienia organu nadzorczego określone w art. 57 i 58 rozporządzenia2016/679, przy czym ich wybór został dokonany z uwzględnieniem specyfiki wymiaru sprawiedliwości oraz konieczności zachowania zasad jego niezależności i niezawisłości.

31. Ustawa z dnia 22 sierpnia 1997 r. o publicznej służbie krwi

W związku z wejściem w życie rozporządzenia 2016/679 powstaje konieczność jednoznacznego wskazania podmiotu odpowiedzialnego za administracje danych osobowych zawartych w systemie e-krew, poprzez wyraźne wskazanie jako administratora tych danych – ministra właściwego do spraw zdrowia.

32. Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych

Zmiana o charakterze czysto technicznym polegająca na usunięciu odesłania w art. 6d ust. 4b do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

33. Ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji

W ustawie o komornikach sądowych i egzekucji projektowane przepisy regulują trzy odrębne zagadnienia i dzielą się na trzy części. Pierwsza dotyczy określenia warunków

przetwarzania danych osobowych przez komorników sądowych, jako podmiotów wykonujących zadania w ramach sprawowania władzy publicznej, polegające na prowadzeniu postępowań egzekucyjnych i zabezpieczających oraz wykonywanie innych zadań przewidzianych w ustawie. Druga dotyczy zadań Ministra Sprawiedliwości jako podmiotu wyposażonego w określone kompetencje wobec komorników sądowych i asesorów komorniczych, związane w szczególności z powoływaniem, odwoływaniem i zawieszaniem w czynnościach komorników. Trzecia wiąże się z zadaniami Ministra Sprawiedliwości oraz innych organów (prezesi sądów, sędziowie wizytatorzy, Krajowa Rada Komornicza i komornicy – wizytatorzy) w zakresie realizacji nadzoru nad działalnością komorników.

Mając na uwadze konieczność sprawnego i niezakłóconego wykonywania przez komorników czynności egzekucyjnych oraz innych powierzonych im zadań, konieczne było wyłączenie stosowania części przepisów ogólnego rozporządzenia o ochronie danych – zgodnie z upoważnieniem wynikającym z art. 23 tego rozporządzenia 2016/679. Dotyczy to w szczególności obowiązków informacyjnych administratora danych osobowych określonych w art. 13-15 ust. 1 i 3, 19 rozporządzenia 2016/679 oraz praw osoby, której dane są przetwarzane określonych w art. 18 i 21 ust. 1 tego rozporządzenia. Konieczność przetwarzania danych osobowych w toku prowadzonego przez komornika postępowania wyklucza również możliwość korzystania przez osobę, której dane są przetwarzane z prawa żądania ograniczenia przetwarzania danych i sprzeciwu wobec ich przetwarzania. Z kolei wykonywanie prawa do sprostowania tych danych (art. 16 rozporządzenia 2016/679) odbywać się musi z zachowaniem przepisów regulujących prowadzone przez komornika postępowanie, tj. przepisów Kodeksu postępowania cywilnego i ustawy o komornikach sądowych i egzekucji.

Komornik został przy tym wskazany jako administrator danych. Natomiast funkcje przepisów dotyczących zabezpieczeń zapobiegających nadużyciom, niezgodnemu z prawem dostępowi lub przekazywaniu spełniają inne przepisy ustawy o komornikach sądowych i egzekucji, w szczególności art. 20 ustawy o komornikach sądowych i egzekucji regulujący tajemnicę komorniczą. Okresy przechowywania dokumentacji zawierającej dane osobowe reguluje art. 37b ustawy o komornikach sądowych i egzekucji i przepisy dotyczące archiwizacji akt wydane na jego podstawie.

Konieczność przetwarzania danych osobowych osób uczestniczących w postępowaniach, w zakresie w jakim dane te są zawarte w prowadzonych przez komorników aktach oraz urządzeniach ewidencyjnych, jest nieodłącznie związane z nadzorem

sprawowanym nad działalnością komorników. Stanowi bowiem nieodłączną część uprawnienia do wglądu w czynności komorników. Stąd też konieczność przyznania określonych uprawnień i wyłączenia stosowanie przepisów rozporządzenia wobec podmiotów wykonujących funkcje nadzorcze.

Wreszcie uprawnienie do przetwarzania danych osobowych komorników i asesorów komorniczych przysługiwać powinno również Ministrowi Sprawiedliwości i organom za pośrednictwem których Minister wykonuje zwierzchni nadzór nad działalnością komorników. W ramach sprawowanego nadzoru organy te są również uprawnione do podejmowania samodzielnych działań wobec komorników i asesorów, wymagających przetwarzania danych osobowych.

34. Ustawa z dnia 29 sierpnia 1997 r. o usługach turystycznych

Zmiany proponowane w ustawie o usługach turystycznych maja na celu jednoznaczne określenie, że przedsiębiorcy prowadzący obiekty hotelarskie, w zakresie swojej działalności i w zakresie uzasadnionym świadczonymi usługami hotelarskimi przetwarzają dane osobowe dotyczące klientów w tym dane osobowe dotycząc zdrowia klientów. Wprowadzenie tej regulacji usankcjonuje działanie zwłaszcza przedsiębiorców prowadzących obiekty hotelarskie, którzy świadczą szeroko rozumiane usługi sanatoryjno-zdrowotne, a jednocześnie nie są oni objęci ustawą z dnia 28 lipca 2005 r. o lecznictwie uzdrowiskowym, uzdrowiskach i obszarach ochrony uzdrowiskowej oraz o gminach uzdrowiskowych.

W punkcie drugim proponuje się ograniczenie stosowania art. 14 rozporządzenia 2016/679. Obiekty hotelarskie bardzo często pozyskują dane osobowe klientów w sposób inny niż od nich samych. Dzieje się tak w szczególności w przypadku zawierania umów o usługi hotelarskie na rzecz klientów przez podmioty trzecie. Należy jednak zauważyć, że stosowanie art. 14 rozporządzenia 2016/679 zostało ograniczone w ten sposób, że obiekty hotelarskie będą zobowiązane do wypełniania obowiązku informacyjnego, o którym mowa w tym artykule najpóźniej w chwili faktycznego rozpoczęcia przez klienta korzystania z usług hotelarskich.

35. Ustawa z dnia 29 sierpnia 1997 – Ordynacja podatkowa

Zmiana w art. 14 polega na rezygnacji z odwołania do pojęcia administratora w rozumieniu ustawy o ochronie danych osobowych.

Propozycja dodania w art. 293 § 3 dopuszcza, w sytuacji przetwarzania danych osobowych objętych tajemnicą skarbową, możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i art. 34 RODO. Ograniczenie praw podmiotów danych jest możliwe na podstawie art. 23 ust. 1 lit. d i e RODO, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym 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 oraz 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. W przypadku dodawanego § 3 ograniczenie to zostało zastosowane w zakresie niezbędnym do realizowania zadań ustawowych przez organy podatkowe.

Przepis zawiera ponadto o 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.

36. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe

Zmiana w art. 4 dotyczy uzupełnienia tzw. słowniczka do ustawy i wynika z konieczności uwzględnienia odwołań do przepisów rozporządzenia 2016/679 w regulacjach ustawy - Prawo bankowe.

Zmiana (dodanie) art. 13c:

W związku ze szczególnym charakterem działalności jaką prowadzą banki i powszechnym korzystaniem z usług finansowych świadczonych przez banki, pożądanym jest zapewnienie adekwatnej ochrony informacji powierzanych podmiotom świadczącym tego typu usługi.

Proponuje się zatem wprowadzenie do przepisów Prawa bankowego postanowień, które dawałyby bankom podstawę prawną do pozyskiwania i przetwarzania danych o niekaralności pracowników zatrudnianych na określonych stanowiskach. Należy wskazać, że w obecnym stanie prawnym przepisy prawa pracy nie dają pracodawcom instrumentów, aby politykę

bezpieczeństwa informacji poufnych wdrażać już na etapie doboru pracowników. Mając na uwadze, że osoby zatrudnione przez banki mają bezpośredni dostęp do danych objętych ochroną, zasadnym jest zachowanie szczególnej ostrożności przy doborze kadry. Intencją regulacji jest zminimalizowanie ryzyka zatrudnienia osoby, która mogłaby mieć zamiar wykorzystania przedmiotowego dostępu w celach nieuczciwych.

Ponadto, w celu zapobieżenia przed dostępem nieuprawnionych osób do informacji przetwarzanych przez bank i pomieszczeń, regulacje w art. 13c stwarzają możliwość żądania od pracownika danych biometrycznych, co pozwoli na kontrolę dostępu do ww. informacji. Należy jednocześnie zwrócić uwagę, że umożliwienie instytucjom finansowym korzystania z nowoczesnych rozwiązań w zakresie identyfikacji pracowników stanowi istotną przesłankę w związku rozwojem nowoczesnych form komunikacji oraz stosowanych zabezpieczeń. Uwzględniając, że banki mogą, w drodze umowy agencyjnej, powierzyć wykonywanie określonych czynności objętych działalnością banku przedsiębiorcom krajowym lub zagranicznym, przewidziano również możliwość żądania informacji dotyczącej niekaralności od osób ubiegających się o zatrudnienie (a także pracowników) u tych przedsiębiorców (art. 13c ust. 4).

Zmiana art. 70 – dodanie ust. 1a:

Obowiązek badania zdolności kredytowej klienta przez banki wynika z przepisów Prawa bankowego. Zakres badania zdolności kredytowej jest określony również w Rekomendacji T i S wydanej przez Komisję Nadzoru Finansowego. KNF dzieli badanie zdolności kredytowej na dwa podstawowe elementy (zasady):

1) badanie zdolności kredytowej w aspekcie ilościowym, czyli badanie zdolności finansowej klienta do obsługi zaciąganego zadłużenia;

2) badanie zdolności kredytowej w aspekcie jakościowym, czyli badanie skłonności klienta do spłaty zadłużenia, nazywane również badaniem wiarygodności kredytowej.

Do prognozy skłonności klienta do spłaty kredytu (wiarygodności kredytowej) wykorzystuje się modele scoringowe, które są modelami statystycznymi, czyli budowanymi z wykorzystaniem metod statystycznych. Oprócz modelu wymagane są dane dotyczące klienta lub jego historii kredytowej, na podstawie których model wylicza ocenę wiarygodności kredytowej danej osoby.

Banki wykorzystują oceny punktowe i modele scoringowe udostępniane przez rejestry kredytowe do podejmowania decyzji kredytowych w indywidualnych przypadkach, również tych odbywających się w procesach automatycznych. Pomimo samodzielnego uprawnienia banków do profilowania klienta w procesie oceny zdolności kredytowej i analizy ryzyka kredytowego, to dopiero modele scoringowe wykorzystywanie przez rejestry kredytowe (przetwarzające dane z całego sektora bankowego) pozwalają na przygotowanie adekwatnej oceny punktowej w procesie kredytowym.

Zmiana art. 70 ustawy – Prawo bankowe polegająca na odwołaniu się wprost do możliwości przetwarzania danych osobowych w drodze profilowania, zagwarantuje bankom możliwość wykorzystywania profilowania w procesie oceny zdolności kredytowej.

Zmiana art. 105 ust. 1 pkt 2 lit. n i ust. 4:

Zmiana art. 105 ust. 1 ma charakter dostosowawczy i związana jest ze zmianą organu właściwego w sprawach ochrony danych osobowych. Natomiast zmiana ust. 4 ma na celu przesądzenie, że uprawnienie do profilowania przysługuje również instytucjom utworzonym na podstawie art. 105 ust. 4 ustawy – Prawo bankowe (rejestrom kredytowym), które gromadzą i udostępniają informacje stanowiące tajemnicę bankową na zasadach określonych w tym przepisie.

Zmiana art. 105a ust. 1:

Zmiana polega na modyfikacji dotychczasowego brzmienia ww. artykułu przede wszystkim poprzez wskazanie, że przetwarzanie danych może obejmować również profilowanie.

Zapis ten jest spójny z innymi przepisami ustawy przyznającymi bankom oraz rejestrom kredytowym uprawnienie do profilowania klienta. Proponuje się zatem przepis art. 105a ust. 1 uzupełnić również o przetwarzanie danych osobowych obejmujące profilowanie.

Uprawnienie do przetwarzania zgromadzonych danych dla celów statystycznych ma istotne znaczenie dla umożliwienia przekazywania obowiązkowych sprawozdań na potrzeby Narodowego Banku Polskiego, Komisji Nadzoru Finansowego i Bankowego Funduszu Gwarancyjnego. Przykładowo, zgodnie z art. 23 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim, banki przekazują NBP m.in.: dane niezbędne do ustalania polityki pieniężnej i okresowych ocen sytuacji pieniężnej państwa oraz na jego żądanie, dane niezbędne do analiz ryzyka systemowego. Natomiast zgodnie z art. 330 ust. 3 ustawy z dnia 10 czerwca

2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji, podmioty objęte systemem gwarantowania (banki) są obowiązane przekazywać Funduszowi informacje inne niż przekazywane do Narodowego Banku Polskiego i do Komisji Nadzoru Finansowego, niezbędne do wykonywania zadań Funduszu, w szczególności informacje o wartości wierzytelności i wartości środków gwarantowanych przez Fundusz oraz dane i informacje niezbędne do wyliczenia obowiązkowych składek, w tym banków. W przypadku Komisji Nadzoru Finansowego, zgodnie z art. 133a 1 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe, Komisja Nadzoru Finansowego co najmniej raz w roku przeprowadza badanie i ocenę nadzorczą banku albo przegląd i weryfikację wyników poprzedniego badania i oceny nadzorczej. W ramach takiego badania i oceny nadzorczej ma prawo otrzymywania od banku wszelkich niezbędnych informacji, także z wykorzystaniem wszelkich zasobów, które bank posiada lub może posiadać jako dane w instytucji utworzonej na podstawie art. 105 ust. 4 Prawa bankowego (w rejestrze kredytowym). Stworzenie wyraźnej podstawy prawnej przetwarzania przez banki, innych kredytodawców oraz rejestry kredytowe zgromadzonych danych do celów statystycznych, pozwala na wypełnienie przesłanek zgodności przetwarzania z prawem, określonych w art. 6 rozporządzenia 2016/679.

Zmiana art. 106d:

Art. 106d dotyczy przetwarzania i udostępniania informacji na potrzeby tzw. Platformy Antyfraudowej. Proponuje się dotychczasowe zapisy dotyczące przetwarzania danych w sposób symetryczny uzupełnić o dokonywanie profilowania.

Przetwarzanie i wymiana danych, o której stanowi przepis art. 106d Prawa bankowego pozwala na zapobieganie przestępstwom popełnianym na szkodę instytucji finansowych i jej klientów (np. posługiwanie się fałszywymi dokumentami czy składanie fałszywych oświadczeń), wzmacniając bezpieczeństwo prowadzonej działalności oraz środków pieniężnych (depozytów) klientów zgromadzonych w tych podmiotach.

Wobec tego, że zasady (reguły) porównywania danych w systemach antyfraudowych opierają się na wystąpieniu określonej cechy/zachowania/czynnika osobowego osoby fizycznej to wydaje się, że te procesy analityczne odpowiadają definicji „profilowania” wprowadzonej przepisami rozporządzenia 2016/679 (art. 4 pkt. 4). Efekty przetwarzania danych przez systemy antyfraudowe wskazują sytuacje, którym kredytodawca powinien się szczególnie przyjrzeć i

dodatkowo zweryfikować (np. osoba, która złożyła wniosek kredytowy w banku lub w innej instytucji udzielającej kredytów posłużyła się dokumentem tożsamości, który został zastrzeżony).

System wymiany danych pomiędzy bankami i instytucjami udzielającymi finansowania (kredyt, leasing) z udziałem rejestru kredytowego i przy wykorzystaniu analiz antyfraudowych opierających się na profilowaniu niewątpliwie przyczynia się do ograniczania ryzyka operacyjnego występującego w podmiotach udzielających kredytów/pożyczek/leasingów i zmniejszenia strat wynikających z przestępstw popełnianych na ich szkodę oraz szkodę ich klientów. Doświadczenia, w tym europejskich biur kredytowych, wskazują na wysoką efektywność systemów antyfraudowych działających na regułach wykrywających korelacje danych.

Postanowienia ust. 2 i 3 określają niezbędne warunki/wyłączenia stosowania rozporzadzenia 2016/679.

Zmiana art. 112b:

Zmiana w ust. 1 ww. artykułu polega na uzupełnieniu dotychczasowego brzmienia o zapis dotyczący uprawnienia banków do przetwarzania danych biometrycznych zdefiniowanych w art. 4 pkt rozporządzenia 2016/679. Dane biometryczne w rozumieniu przepisów rozporządzenia 2016/679 oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

W regulacjach art. 112b ust. 1, który stanowi podstawę przetwarzania danych biometrycznych określa się równocześnie cele, w jakich banki mogą przetwarzać te dane, tj. w celu zidentyfikowania lub weryfikacji tożsamości osoby fizycznej, a także uwierzytelnienia czynności dokonywanej przez osobę fizyczną. Należy wskazać, że biometria stanowi coraz istotniejszą kwestię uwzględnianą w praktyce funkcjonowania sektora bankowego, w szczególności przy świadczeniu przez banki usług płatniczych oraz przy stosowaniu systemów bezpieczeństwa systemów bankowych. Biometria wykorzystywana jest przede wszystkim w zakresie tzw. silnej weryfikacji uwierzytelniania klienta. Przyjmuje się, że najnowsze systemy biometryczne należą do jednych z najbardziej wiarygodnych i niezawodnych metod identyfikacji/weryfikacji osoby. Wskazać warto, że dyrektywa Parlamentu Europejskiego i

Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, przewiduje wykorzystywanie danych biometrycznych na potrzeby silnego uwierzytelnienia klienta.

Biorąc pod uwagę fakt, że dane biometryczne są uznawane za dane wrażliwe zgodnie z art. 9 rozporządzenia 2016/679, proponuje się wyraźne wskazanie w jakich przypadkach/celach banki mogą przetwarzać dane biometryczne.

W art. 112b ust. 2 przewidziano możliwość przetwarzania danych biometrycznych również przez instytucje utworzone na podstawie art. 105 ust. 4 ustawy – Prawo bankowe, w celu identyfikacji lub weryfikacji tożsamości osoby fizycznej. Przetwarzanie danych biometrycznych przez rejestry kredytowe pozwala na wzmocnienie bezpieczeństwa gromadzonych i udostępnianych informacji przez rejestry kredytowe oraz powinno przyczynić się do zmniejszenia zjawiska tzw. kradzieży tożsamości.

Sposób przetwarzania danych biometrycznych zostanie określony w rozporządzeniu Ministra Cyfryzacji wydanym na podstawie delegacji w art. 112b ust. 3 ustawy.

Zmiana (dodanie) art. 112e:

Art. 23 rozporządzenia 2016/679 daje możliwość ograniczenia zakresu obowiązków administratora i podmiotu przetwarzającego, wynikających z rozporządzenia 2016/679, o ile zakłada to prawo UE bądź państwa członkowskiego. Przepis art. 23 rozporządzenia 2016/679 określa jednocześnie jakim celom służyć ma przepis ograniczający odnośne obowiązki..

Proponuje się, aby w stosunku do banków zastosować ograniczenia obowiązków nałożonych na administratora danych osobowych poprzez wprowadzenie art. 112e Prawa bankowego, w projektowanym brzmieniu.

Należy wskazać, iż obowiązki administratora podlegające ograniczeniu bądź wyłączeniu dotyczą obowiązków informacyjnych, obowiązków wykonania prawa do bycia zapomnianym, czy prawa do przenoszalności danych, ale także obowiązki notyfikacji naruszenia bezpieczeństwa danych wobec podmiotów danych osobowych.

Wśród projektowanych ograniczeń obowiązków nałożonych na administratorów, będących bankami, wymienić m.in. należy:

- ograniczenie prawa do dostępu do danych oraz prawa do informacji dotyczących profilowania w zakresie realizacji ustawowych obowiązków banków przeciwdziałania oszustwom i innym przestępstwom, praniu pieniędzy i finansowaniu terroryzmu;

- ograniczenie katalogu sytuacji, w których bank obowiązany jest dokonywać notyfikacji naruszenia bezpieczeństwa danych osobowych wobec osób, których dane dotyczą (art. 34 rozporządzenia 2016/679), w przypadku gdy taka notyfikacja mogłaby spowodować naruszenie stabilności funkcjonowania banku jako instytucji finansowej;

W sytuacji, w której rejestr kredytowy byłby zobowiązany do wykonania prawa do przenoszenia danych (art. 20 rozporządzenia 2016/679) istotne jest, aby temu prawu nie podlegały dane stanowiące tajemnicę przedsiębiorstwa, w szczególności informacje dotyczące wierzycieli (kredytodawców). Prowadzone w aktualnym stanie prawnym i faktycznym systemy wymiany informacji kredytowej, oparte na podstawie ustawowej, tj. art. 105 ust. 4 ustawy Prawo bankowe, ale również na podstawie umów zawieranych z bankami, jako zasadę przyjmują, iż informacje udostępniane ze zbioru rejestru kredytowego – na zasadzie wzajemności – innym bankom lub instytucjom upoważnionym do udzielania kredytów nie będą umożliwiały identyfikacji banku, a więc tych podmiotów, które przekazały dane kredytobiorców do rejestru kredytowego. Zasada nieujawniania informacji dotyczących wierzycieli (zasada neutralności) zapewnia konkurencyjność wśród banków i innych kredytodawców, ponieważ otrzymują one jedynie informacje o historii kredytowej klienta. Poza tym nieujawnianie danych wierzyciela służy także ochronie polityki kredytowej banku, która objęta jest tajemnicą przedsiębiorstwa. Mając powyższe na względzie, w projektowanym art. 112e ust. 2 wprowadzono ograniczenie, iż uprawnienie do przenoszenia danych (art. 20 rozporządzenia 2016/679) nie dotyczy przenoszenia danych stanowiących tajemnicę przedsiębiorstwa.

37. Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej - Komisji Ścigania zbrodni przeciwko Narodowi Polskiemu

Zmiany dokonywane w ustawie mają gównie charakter porządkowy. Zmiana dokonywana w pkt 1 ma na celu usunięcie odesłania do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, która to ustawa zostanie uchylona. W jej miejsce obowiązywać będzie nowa ustawa o ochronie danych osobowych oraz rozporządzenie 2016/679.

W punkcie drugim postanowiono uchylić ust. 3 w art. 53h ustawy o Instytucie Pamięci Narodowej - Komisji Ścigania zbrodni przeciwko Narodowi Polskiemu. Zgodnie z tą regulacją w przypadku wykreślenia bazy materiału genetycznego lub bazy materiału biologicznego z rejestru zbiorów danych osobowych, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, podmiot będący administratorem tej bazy przekazuje do Instytutu Pamięci informacje i dane oraz posiadane próbki materiału genetycznego i biologicznego. Regulację tę należało uchylić z tego względu, iż od 25 maja 2018 r. czyli z dniem w którym zacznie być bezpośrednio stosowane rozporządzenie 2016/679 nie będzie istniał obowiązek rejestracji zbiorów danych, nie zaistnieje zatem sytuacja wykreślenia takiego zbioru danych z rejestru prowadzonego obecnie przez Generalnego Inspektora Ochrony Danych Osobowych, zatem norma zawarta w ust. 3 w art. 53h nie będzie mogła zostać zrealizowana.

W punkcie trzecim zawarto regulacją, która ma na celu dostosowanie obecnego brzmienia art. 71 do regulacji zawartych w rozporządzeniu 2016/679. Zgodnie z obecnym brzmieniem art. 71 w działalności Instytutu Pamięci Narodowej, z wyjątkiem prowadzenia Bazy materiału Genetycznego, nie stosuje się przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Regulację tą należy uznać za niezgodną z rozporządzeniem 2016/679, które wyraźnie wskazuje cel oraz możliwy do zastosowania zakres wyłączenia przepisów rozporządzenia. Analizując rozporządzenie 2016/679 uznano, że w przypadku działalności realizowanej przez Instytut pamięci Narodowej należy skorzystać z możliwości wyłączenia przepisów rozporządzenia przewidzianej w art. 89 ust. 3 rozporządzenia 2016/679. Zgodnie z art. 89 ust. 3 rozporządzenia 2016/679 w przypadku przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, prawo państwa członkowskiego może przewidzieć wyjątki od praw, o których mowa w art. 15, 16, 18, 19, 20 i 21. W zaproponowanym brzmieniu art. 71 postanowiono skorzystać z całego możliwego katalogu włączeń.

38. Ustawa z dnia 21 maja 1999 r. o broni i amunicji

Propozycje zmian opierają się na założeniu, że materialne regulacje nowej ustawy będą ograniczone jedynie do kwestii, które zostały przez prawodawcę unijnego wprost przekazane do uregulowania w prawie krajowym oraz takich, w których rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego

przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) pozostawiło pewną swobodę regulacyjną prawodawcy krajowemu.

Należy podkreślić, że proponowane regulacje prawne są konieczne zważywszy na zobowiązania nałożone na państwa członkowskie Unii Europejskiej do przestrzegania przepisów rozporządzenia 2016/679.

Mając na uwadze zasadę generalną, że umocowanie podmiotu do przetwarzania danych osobowych powinno być uregulowane w akcie rangi ustawowej w zaproponowanym brzmieniu przepisów dokonano takich zmian.

W art. 27 ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2012 r. poz. 576, z późn. zm.) zawarto upoważnienie dla Żandarmerii Wojskowej do przetwarzania informacji, w tym danych osobowych w ramach prowadzonych postepowań o pozwolenia na broń oraz czynności kontrolnych, o których jest mowa w powołanym powyżej akcie prawnym, w celu realizacji ustawowych zadań. W powołanym wyżej przepisie wskazano właściwość miejscową komendantów Oddziałów ŻW -jako administratorów tych danych osobowych, wynikającą z miejsca stałego pobytu wnioskodawcy w sprawach pozwoleń na broń. Wskazano również, że przedmiotowe dane osobowe stanowią tajemnicę prawnie chronioną i podlegają ochronie przewidzianej dla informacji o klauzuli tajności „zastrzeżone” określonej w przepisach o ochronie informacji niejawnych.

39. Ustawa z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka

Dokonywana zmiana ma charakter dostosowujący. Po pierwsze, obowiązujące przepisy w zakresie ochrony danych osobowych - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) - zostaną uchylone. Odwołania zawarte w ustawie o Rzeczniku Praw Dziecka do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych musiały więc zostać dostosowane do nowej sytuacji prawnej.

Po drugie, art. 9 rozporządzenia 2016/679 wskazuje na przesłanki przetwarzania danych osobowych wrażliwych. Spośród wszystkich przewidzianych w rozporządzeniu, do Rzecznika Praw Dziecka mogłaby znaleźć zastosowanie - oprócz art. 9 ust. 2 lit. a, c, e lub f - również art. 9 ust. 2 lit. g, tj. gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego. Konstrukcja tej przesłanki może rodzić poważne wątpliwości interpretacyjne, czy norma kompetencyjna stanowiąca wyraźnie o przetwarzaniu danych musi znaleźć się w ustawie, czy

też wystarczającym byłoby, by ustawa przewidywała zadanie, dla którego realizacji konieczne jest przetwarzanie danych. Z tego względu, uwzględniając konieczność utrzymania dotychczasowych kompetencji Rzecznika Praw Dziecka do przetwarzania danych osobowych dla skutecznego wykonywania jego ustawowych zadań, zdecydowano się wprowadzić przepis upoważniający do przetwarzania danych osobowych wrażliwych. Jednocześnie wskazano, że uprawnienie to znajduje zastosowanie wyłącznie w celu ochrony praw dziecka i przy realizacji przez Rzecznika jego ustawowych zadań.

Uwzględniając powyższe, zmiana w art. 10c ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Dziecka związana jest po pierwsze z uchyleniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dotychczasowe brzmienie art. 10c ustawy o Rzeczniku Praw Dziecka przyznawało podstawę prawną do przetwarzania wszelkich danych osobowych, w tym danych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych niezbędnych do realizacji ustawowych zadań Rzecznika. Po drugie, zmiana wynika z brzmienia art. 9 rozporządzenia 2016/679.

40. Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym

Zmiana art. 4 ust. 2 ustawy o Krajowym Rejestrze Karnym ma na celu usunięcie odwołania do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, która zostanie uchylona w związku z wejściem w życie rozporządzenia 2016/679. Z racji istnienia definicji legalnej administratora danych w ww. rozporządzeniu, nie jest konieczne precyzowanie, że Minister Sprawiedliwości pełni tę funkcję w rozumieniu innego aktu.

W art. 4 ust. 3 ustawy o Krajowym Rejestrze Karnym przewiduje się wyłączenie stosowania przepisów art. 18 (prawo do ograniczenia przetwarzania), art. 19 (obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych) i art. 21 (prawo do sprzeciwu) rozporządzenia 2016/679.

Ograniczenie ww. praw i obowiązków w stosunku do danych przetwarzanych w KRK jest niezbędne dla zapewnienia ciągłości funkcjonowania i sprawności tego Rejestru, które służy bezpieczeństwu publicznemu, zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar, a także funkcjom kontrolnym, inspekcyjnym i regulacyjnym związanym ze sprawowaniem władzy publicznej.

Bezwzględne egzekwowanie prawa do ograniczenia przetwarzania danych lub prawa do wniesienia sprzeciwu wobec przetwarzania danych mogłoby doprowadzić do uniemożliwienia przetwarzania danych poprzez udzielanie informacji o osobie z KRK. To z kolei zagrażałoby realizacji ww. zadań, realizowanych w interesie publicznym.

Jednocześnie istniejące regulacje zapewniają odpowiednią ochronę praw i wolności osób w tym zakresie. Zgodnie z przepisem art. 18 ust. 1 ustawy o Krajowym Rejestrze Karnym, w przypadku stwierdzenia okoliczności wskazujących na prawdopodobieństwo wprowadzenia do Rejestru nieprawidłowych danych osobowych, przeprowadza się postępowanie w celu ustalenia prawidłowych danych. Postępowanie to nie wyklucza jednak możliwości dalszego przetwarzania tych danych w postaci udzielania informacji z KRK (gdy podejrzenie dotyczy nieprawidłowości nieistotnych danych). Natomiast możliwość wcześniejszego zatarcia skazania na karę pozbawienia wolności na mocy postanowienia sądu wydanego na wniosek skazanego (art. 107 § 2 k.k.), a także zatarcia skazania na mocy prawa łaski Prezydenta Rzeczypospolitej Polskiej zabezpieczają interesy osoby do zaprzestania przetwarzania danych dotyczących jej karalności z przyczyn związanych z jej szczególną sytuacją.

Stosowanie obowiązku powiadomienia o sprostowaniu danych osobowych wszystkich odbiorców, którym ujawniono dane (art. 19 rozporządzenia 2016/679) stanowiłoby nadmierny ciężar, zagrażający efektywności działania KRK. Nie znajduje on ponadto uzasadnienia w kontekście informacji udzielanych z KRK. Odpowiednie zabezpieczenie praw i wolności osób w tym zakresie stanowi przepis art. 18 ust. 3 ustawy o Krajowym Rejestrze Karnym, przewidujący zawiadomienie o sprostowaniu danych strony, tj. podmiotu wnioskującego o sprostowanie.

W art. 8 ust. 3a ustawy o Krajowym Rejestrze Karnym przewidziano dodatkowe wyłączenie określonych przepisów ogólnego rozporządzenia o ochronie danych w odniesieniu do szczególnej kategorii danych osobowych przetwarzanych w KRK – danych przetwarzanych do badań naukowych i do celów statystycznych. Zakłada się wyłączenie stosowania przepisów art. 15 ust. 1 (prawo dostępu przysługujące osobie, której dane dotyczą) i 16 (prawo do sprostowania danych), art. 18 (prawo do ograniczenia przetwarzania) i art. 21 (prawo do sprzeciwu) rozporządzenia 2016/679. Stosowanie tych praw uniemożliwiłoby, a przynajmniej znacznie utrudniłoby, przekazywanie danych zgromadzonych w Rejestrze do badań naukowych i do celów statystycznych. Przetwarzanie danych do tych celów jest zarazem uregulowane rozporządzeniem Ministra Sprawiedliwości z dnia 1 lipca 2015 r.

w sprawie szczegółowych zasad i sposobu przetwarzania oraz przekazywania danych osobowych zgromadzonych w zbiorach Krajowego Rejestru Karnego do celów statystycznych oraz badań naukowych (Dz. U. z 2015 r. poz. 984). Rozporządzenie to odpowiednio zabezpiecza prawa i wolności osób, których dane dotyczą, zgodnie z ogólnym rozporządzeniem o ochronie danych.

41. Ustawa z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych

Wprowadzana zmiana ma cel doprecyzowujący. Jej istotą jest wskazanie na rolę ujętego w nim podmiotu jako na administratora danych.

42. Ustawa z dnia 3 lutego 2001 r. o ochronie dziedzictwa Fryderyka Chopina

W projektowanych zmianach ustawy z dnia 3 lutego 2001 r. o ochronie dziedzictwa Fryderyka Chopina (Dz. U. poz. 168) uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679, który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj przetwarzanych danych osobowych ww. ramach realizacji zadania ustawowego.

Z tego względu zaproponowano zmiany, określające zarówno zakres danych przetwarzanych w związku z przyznaniem odznaki „Zasłużony dla Ochrony Dziedzictwa Fryderyka Chopina", jak i zasady prowadzenia stosownej ewidencji. Z uwagi na fakt, że w obecnym stanie prawnym, zasadnicza część regulacji związanej z przyznawaniem odznaki znajduje się w akcie wykonawczym, wprowadzenie przepisu określającego zakres przetwarzanych danych wymagało przeniesienia części unormowań z aktu wykonawczego bezpośrednio do ustawy. W zakresie samych zasad przyznawania odznaki, w stosunku do stanu obecnego, nie przewiduje się zmian.

Wprowadzono także możliwość zlecenia innym podmiotom przez administratora danych osobowych w celach związanych z ochroną zabytków przetwarzania danych osobowych na jego rzecz oraz pełnienie przez administratora danych osobowych funkcji przetwarzającego dane na zlecenie innego podmiotu.. Jednocześnie proponuje się wskazanie 80-letniego okresu przechowywania danych osobowych w związku z przyznaniem odznaki. W pozostałym zakresie okres ten byłby zależny od realizacji celu przetwarzania.

Na podstawie art. 23 rozporządzeniem 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzeniem 2016/679, w ten sposób, że

korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: Administratorzy danych osobowych, w tym Instytut, jako podmioty publiczne realizujące zadania ustawowe w ramach środków, w tym dotacji z budżetu pąństwa, narażone byłby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzeniem 2016/679 zobowiązując administratora danych osobowych do umieszczenia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej komunikatu o zaistniałym naruszeniu nie później niż 72 godziny od stwierdzenia naruszenia.

Prawa określone w art. 14 rozporządzeniem 2016/679 (prawo do informacji w przypadku, gdy dane pochodzą od osoby trzeciej) oraz obowiązek poinformowania odbiorców o sprostowaniu danych byłyby ograniczone tylko do przypadków, gdy administrator danych osobowych zbiera dane od podmiotów wnioskujących o przyznanie odznaki. Jednocześnie wprowadza się dodatkowy obowiązek poinformowania przez administrator danych osobowych na swojej stronie podmiotowej w Biuletynie Informacji Publicznej o ograniczeniach j.w.

43. Ustawa z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów

Zmiana o charakterze technicznym polegająca na usunięciu odesłania do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

44. Ustawa z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego

Wprowadzana zmiana ma cel doprecyzowujący. Jej istotą jest wskazanie na rolę ujętego w nim podmiotu jako na administratora danych

45. Ustawa z dnia 21 czerwca 2001 r. o dodatkach mieszkaniowych

Wprowadzana zmiana ma cel doprecyzowujący. Jej istotą jest wskazanie na rolę ujętego w nim podmiotu jako na administratora danych.

46. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych

W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2016 r. poz. 1483 i 1948) zmieniono przepisy art. 9 poprzez usunięcie w nim ust. 1a, który przeniesiono do nowoutworzonego art. 8a . W skutek dodania art. 8a ŻW posiada umocowanie w ustawie do przetwarzania danych osobowych w zakresie przeprowadzonych postępowań kwalifikacyjnych. Należy wskazać, że istotą interwencji legislacyjnej mającej doprowadzić do zastosowania RODO w prawie wewnętrznym państw członkowskich jest podniesienia do rangi ustawowej wszystkich przepisów krajowych dotyczących gromadzenia danych osobowych, w tym również gromadzenia danych osobowych w ramach prowadzonych postepowań kwalifikacyjnych do ŻW, dla zagwarantowania im należytej ochrony prawnej. Obecnie regulacje te mają miejsce w akcie wewnętrznym tj. decyzji nr 65/MON Ministra Obrony Narodowej z dnia 4 marca 2009 r. w sprawie postępowania kwalifikacyjnego wobec kandydatów do służby i pracy w Żandarmerii Wojskowej (Dz. Urz. Min. Obr. Nar. poz. 57, z późn. zm.). Ranga aktu prawa wewnętrznego, w myśl RODO jest niewystarczająca toteż nowoutworzone przepisy art. 8a wypełniają obowiązek narzucony przez prawodawcę unijnego.

Stosownie do brzmienia art. 23 RODO, w art. 8a ust. 9 projektu dokonano ograniczeń w zakresie stosowania przepisów art. 5 ust. 2, art. 15 ust. 3 oraz art. 34 RODO.

Odnośnie ograniczenia w stosowaniu art. 5 ust. 2 RODO należy wskazać, że sposób zabezpieczeń informacji, w tym danych osobowych w niejawnych systemach teleinformatycznych jest zawarty w Szczególnych Wymaganiach Bezpieczeństwa, które są dokumentami niejawnymi. Informacje te są zawarte w akredytowanym systemie teleinformatycznym, spełniają przepisy kancelaryjne, oraz są zgodnie z planem ochrony kompleksu wojskowego. Wykazanie przez Żandarmerie Wojskową przestrzegania przepisów art. 5 ust. 1 RODO w sposób oczywisty negatywnie wpłynie na bezpieczeństwo narodowe poprzez ukazanie sposobu doboru żołnierzy do służby w Żandarmerii Wojskowej. Toteż nie wskazane jest przekazywanie szczegółowych informacji o zabezpieczeniach wprowadzonych przez ŻW w ramach postępowań kwalifikacyjnych do ŻW.

Odnośnie ograniczenia stosowania obowiązku nałożonego na Administratora w art. 15 ust. 3 RODO w zakresie dostarczenia osobie, której informacje dotyczą, danych osobowych podlegających przetwarzaniu przez właściwy organ należy wskazać, że to środek niezbędny i proporcjonalny służący bezpieczeństwu narodowemu. Brak nałożenia tego ograniczenia

ujawniło by sposób selekcji kandydatów do służby i pracy w ŻW oraz mogłoby posłużyć do identyfikacji osób biorących udział w procesie kwalifikacyjnym.

Natomiast obwiązek zawiadomienia osoby, której dane dotyczą, o naruszenie ochrony danych osobowych nie powinien mieć zastosowania w stosunku do postępowań kwalifikacyjnych ponieważ ŻW jako wyspecjalizowana służba ma wdrożone własne środki eliminujące prawdopodobieństwo naruszenia informacji państwowych, w tym danych osobowych. Żandarmeria Wojskowa posiada opracowane procedury postępowania na wypadek wystąpienia ewentualnego ataku teleinformatycznego. Informowanie osób fizycznych o ewentualnym naruszeniu ochrony ich danych osobowych mogłoby realnie wpłynąć na obniżenie obronności Rzeczypospolitej Polskiej poprzez ujawnienie okresu osłabienia ochrony teleinformatycznej w zakresie informacji nie objętych atakiem.

Zaproponowano również przeredagowanie art. 29 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, w taki sposób aby sprostać wymogom rozporządzenia RODO. Zmienione przepisy pozwolą Żandarmerii Wojskowej w ramach wykonywanych zadań ustawowych na przetwarzanie danych osobowych, a także zapewnią gromadzonym danym odpowiedni poziom ochrony. Propozycje zmian dotyczą jedynie uregulowania statusu baz danych oraz podstawy prawnej uzyskiwania danych osobowych od instytucji państwowych w toku prowadzonych czynności przedprocesowych .

Wskazane zmiany nie spowodują żadnych dodatkowych skutków finansowych dla resortu obrony narodowej ponieważ przedmiotowe dane osobowe obecnie są już przetwarzane w zakresie niezbędnym do wykonywania ustawowych zadań przez ŻW.

47. Ustawa z dnia 6 września 2001 r. o transporcie drogowym

W ustawie o transporcie drogowym wprowadza się nowy art. 55a, który przewiduje uregulowanie kwestii gromadzenia i przetwarzania danych osobowych przez Inspekcję Transportu Drogowego w zakresie niezbędnym do realizacji jej zadań ustawowych.

Rozwiązania zawarte w projektowanym przepisie oparto na brzmieniu art. 22a ustawy dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2016 r. poz. 1310, z późn. zm.) z uwzględnieniem specyfiki organizacji Inspekcji Transportu Drogowego, która realizuje swoje ustawowe zadania za pośrednictwem różnych organów: Głównego Inspektora Transportu Drogowego oraz wojewódzkich inspektorów transportu drogowego. Wyłączenie obowiązku informowania przez Inspekcję o przetwarzaniu danych osobowych jest zgodne z

art. 23 rozporządzenia 2016/679. Inspekcja sprawuje bowiem funkcje kontrolne, inspekcyjne i regulacyjne związane ze sprawowaniem władzy publicznej służącym bezpieczeństwu publicznemu (zapewnianie bezpieczeństwa ruchu drogowego) oraz innym ważnym celom leżącym w ogólnym interesie publicznym (m. in. kontrola przewozów drogowych, kontrola prawidłowości uiszczenia opłaty elektronicznej).

W odniesieniu do zmian w art. 82 ustawy o transporcie drogowym i wyłączenia przepisu art. 14 RODO należy zauważyć, że przepis ten jest wymagany ze względu na skalę prowadzonych postępowań kontrolnych przez organy Inspekcji Transportu Drogowego w zakresie warunków i obowiązków wykonywania transportu drogowego, przewozu drogowego towarów niebezpiecznych, pojazdów nienormatywnych oraz obowiązku uiszczenia opłaty elektronicznej za przejazd po drogach krajowych. Pozyskiwanie danych osobowych jest wymagane ze względu na realizację zadań ustawowych i egzekucję przepisów prawa unijnego i krajowego z zakresu przewozów drogowych i opłaty elektronicznej.

48. Zmiany w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną zwana dalej „uśude" w zakresie przesyłania informacji handlowych za pomocą środków komunikacji elektronicznej stanowi implementację dyrektywy 2002/58[1]. Art. 13 ust. 1 dyrektywy 2002/58 wskazuje, iż używanie automatycznych systemów wywołujących bez ludzkiej ingerencji (aparaty wywołujące automatycznie), faksów lub poczty elektronicznej do celów marketingu bezpośredniego może być dozwolone jedynie wobec abonentów, którzy uprzednio wyrazili na to zgodę. W tym kontekście należy zwrócić uwagę, iż dyrektywa 2002/58 nie zawiera samodzielnej definicji zgody na przesyłanie informacji handlowej za pomocą środków komunikacji elektronicznej i w tym zakresie odwołuje się do dyrektywy 95/46. Zgodnie z motywem 17 dyrektywy 2002/58 „Do celów niniejszej dyrektywy, zgoda użytkownika lub abonenta, niezależnie od tego czy abonentem jest osoba fizyczna czy prawna, powinna mieć to samo znaczenie co zgoda podmiotu danych opisana i szerzej określona w dyrektywie 95/46/WE. Zgoda może być udzielona w jakikolwiek sposób umożliwiający

[1] 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).

swobodne i świadome wyrażenie woli użytkownika, włączając zaznaczenie okna wyboru podczas przeglądania witryny internetowej".

W kontekście powyższego należy zwrócić uwagę, iż zgodnie z treścią art. 94 ust. 1 rozporządzenia 2016/679 „Dyrektywa 95/46/WE zostaje uchylona ze skutkiem od dnia 25 maja 2018 r. W związku z tym należy w ramach treści art. 4 uśude odwołać się do treści rozporządzenia 2016/679 - definicja zgody zamieszczona w art. 4 uśude powinna uwzględnić zmianę kontekstu systemowego. W konsekwencji zmiany wymaga obecny art. 4 oraz art. 10 uśude.

Co istotne, zmiana w treści art. 10 ust. 2 uśude ma charakter wyłącznie porządkujący. Wobec odwołania się (w art. 4 uśude w nowym brzmieniu) do definicji zgody w rozumieniu przyjętym w rozporządzenia 2016/679, dookreślanie sposobu jej wyrażenia w art. 10 ust. 2 uśude stało się bezprzedmiotowe. Nie mniej z całą mocą należy podkreślić, iż zmiana art. 10 ust. 2 uśude nie oznacza, iż taki sposób wyrażenia zgody jest sprzeczny z treścią rozporządzenia 2016/679.

Odwołanie się do przepisów o ochronie danych osobowych w treści art. 4 uśude (w nowym brzmieniu) oznacza, iż zastosowanie znajdą w szczególności przepisy art. 4 ust. 11, art. 7 oraz 8 rozporządzenia 2016/679 a także art. 3 projektowanej ustawy o ochronie danych osobowych realizujący kompetencję wskazaną w art. 8 ust. 1 *in fine* rozporządzenia 2016/679 w zakresie zgody dziecka.

Rozporządzenie 2016/679 swoim zakresem podmiotowym i przedmiotowym obejmuje przetwarzanie danych osobowych związku ze świadczeniem usług drogą elektroniczną (regulowanych treścią uśude). Jednocześnie ogólne rozporządzenie nie daje podstaw do doprecyzowania lub zawężenia jego przepisów w zakresie i w sposób jaki ma to miejsce obecnie w rozdziale IV uśude. W związku z tym należy w rozdziale IV uśude uchylić przepisy dotyczące materii regulowanych treścią rozporządzenia 2016/679.

W treści rozdziału IV należało pozostawić wyłącznie dwie kategorie przepisów:

- implementujące dyrektywę 2002/58 a to ze względu na treść art. 95 rozporządzenia 2016/679 („Niniejsze rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie

2002/58/WE") a także motywu (173) rozporządzenia 2016/679: „Niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich tych kwestii dotyczących ochrony podstawowych praw i wolności w związku z przetwarzaniem danych osobowych, które nie podlegają szczególnym obowiązkom mającym ten sam cel określonym w dyrektywie Parlamentu Europejskiego i Rady2002/58/WE (2), w tym obowiązkom nałożonym na administratora oraz prawom osób fizycznych. Aby doprecyzować związek między niniejszym rozporządzeniem a dyrektywą 2002/58/WE, dyrektywę tę należy odpowiednio zmienić (…)".

Powyższe dotyczy obecnego art. 18 ust. 5 uśude (z koniecznymi zmianami w związku z uchyleniem art. 18 ust. 1-4 uśude).

- regulacji nienaruszających ogólnego rozporządzenia i nieobjętych jego treścią.

Dotyczy to obecnego art. 18 ust. 6 oraz art. 19 ust. 3 uśude.

Co istotne, uchylenie w rozdziale IV uśude poszczególnych przepisów nie może być traktowane jako zakaz przetwarzania danych osobowych (w związku ze świadczeniem usług drogą elektroniczną) w sposób określony w tych przepisach albo tym bardziej dopuszczenie przetwarzania tych danych w sposób dowolny. Legalność takiego przetwarzania danych osobowych oceniać należy w świetle przepisów rozporządzenia 2016/679, w tym przede wszystkim zasad ogólnych określonych w art. 5 tej regulacji.

49. Ustawa z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych

Ubezpieczeniowy Fundusz Gwarancyjny („UFG" lub „Fundusz"), wykonuje zadania wynikające z ustawy o UFG, takie jak likwidacja szkód, wypłata odszkodowań, dochodzenie roszczeń związanych z ubezpieczeniami, o których mowa w art. 4 ustawy o UFG, pełnienie funkcji ośrodka informacji (art. 102) i prowadzenie Bazy Danych Ubezpieczeniowych (art. 102a). Dodanie ust. 6 do art. 98 ma na celu jednoznacznie wskazane podstawy prawnej oraz celu przetwarzania danych w związku z wykonywaniem przez Fundusz zadań ustawowych.

Wskazane przepisy ustawy nakładają na UFG obowiązki, z którymi wiąże się konieczność przetwarzania danych osobowych. Rozporządzenie 2016/679 w art. 6 ust. 1 określa podstawy prawne przetwarzania danych osobowych, w tym lit. c, przesłankę stanowiącą, że administrator jest zobowiązany do przetwarzania danych w celu wypełnienia

ciążącego na nim obowiązku prawnego. Jednocześnie, art. 6 ust. 3 rozporządzenia 2016/679 nakazuje aby przesłanka obowiązku prawnego była wyraźnie określona w prawie państwa członkowskiego. Przepisy krajowe powinny także określać co najmniej cel takiego przetwarzania. Proponowana modyfikacja jest zatem uzasadniona ze względu na konieczność wyraźnego wskazania obowiązków jakie ciążą na Funduszu, a w związku z którymi konieczne jest przetwarzanie danych osobowych oraz konieczność doprecyzowania celów przetwarzania danych w związku z wykonywaniem przez UFG wymienionych zadań.

Ponadto, UFG przetwarza szczególne kategorie danych, opisane w art. 9 ust. 1 oraz art. 10 rozporządzenia 2016/679, tj. dane dotyczące stanu zdrowia, a także dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa. W przypadku tych danych należy osobno wskazać, jakie przepisy ustawy o UFG stanowić będą podstawę ich przetwarzania. Nie wszystkie bowiem zadania UFG wymagają przetwarzania szczególnych kategorii danych, natomiast możliwość ich wykorzystania przez UFG musi być wskazana wprost.

Zatem propozycja dodania do art. 98 ust. 7 jest uzasadniona ze względu na konieczność doprecyzowania regulacji ustawowej w odniesieniu do zakresu i celu przetwarzanych szczególnych kategorii danych osobowych w celu oceny wykonywania przez UFG swoich zadań ustawowych.

Zgodnie z art. 10 rozporządzenia 2016/679, przetwarzanie danych o wyrokach skazujących powinno mieć nie tylko wyraźną podstawę w przepisach prawa, ale również dodatkowo zabezpieczone jeśli chodzi o prawa i wolności podmiotów danych. Takim zabezpieczeniem będzie wyraźne objęcie UFG tajemnicą ubezpieczeniową w przepisach ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

Odnosząc się do propozycji dodania art. 98a i 98b należy wskazać, że UFG jest instytucją utworzoną w drodze ustawowej. Fundusz w przeważającym stopniu wykonuje zadania o charakterze publicznym. Fundusz nastawiony jest na osiąganie celów innych niż maksymalizacja zysków, w szczególności jest właściwy w zakresie egzekucji administracyjnej należności pieniężnych w związku z kontrolą zawierania umów obowiązkowych ubezpieczeń odpowiedzialności cywilnej oraz w zakresie zaspokajania roszczeń z tytułu ubezpieczeń obowiązkowych. Z uwagi na obowiązkowy charakter ubezpieczeń, Fundusz realizuje wspomniane zadania w wymiarze ogólnospołecznym. Fundusz został wyposażony w elementy

władztwa publicznego, np. wystawia tytuł wykonawczy w trybie egzekucji administracyjnej w zakresie egzekucji należności w stosunku do podmiotów naruszających obowiązek zawarcia umowy ubezpieczenia OC komunikacyjnego i OC rolników. Fundusz jest ponadto podmiotem niekomercyjnym i w tym znaczeniu ma charakter instytucji non profit.

Rozporządzenie w art. 23 dopuszcza możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i 34, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym m.in.:

• 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;

• 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.

W zakresie ograniczenia prawa wskazanego w art. 12 rozporządzenia 2016/679, dotyczącego przejrzystej i „wszelkiej" komunikacji z podmiotem danych, należy na wstępie zauważyć, iż motyw 62 preambuły rozporządzenia 2016/679 wyraźnie wskazuje, iż ograniczenie obowiązków informacyjnych wobec podmiotów danych jest w szczególności możliwe wtedy, kiedy przetwarzanie danych ma miejsce na podstawie przepisów prawa, podmiot danych dysponuje informacjami dotyczącymi szczegółów operacji przetwarzania danych lub wykonanie obowiązku wobec podmiotów danych wymagałoby niewspółmiernie dużego wysiłku.

W motywie tym podkreśla się, że „sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia."

Z kolei motyw 63 stwierdza, że „każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego

prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (…).”

Należy zauważyć, iż wymienione w motywie 62 przesłanki nie muszą być spełnione łącznie, jednak w przypadku UFG niewątpliwe możliwe jest wykazanie większości okoliczności zwalniających z konieczności wykonywania wspomnianego obowiązku.

Należy jednocześnie wyjaśnić, iż celem proponowanych przepisów art. 98a i 98b nie jest wyłączenie obowiązku związanych ze wskazania podstawowych informacji na temat przetwarzania danych, o których mowa w art. 13 i 14 rozporządzenia 2016/679 które są spełnione przed przekazaniem danych do UFG. Ograniczenie wprowadzone proponowanym art. 98a ma jedynie na celu ograniczenie możliwości korzystania w szczególności z prawa dostarczenia dodatkowych wyjaśnień w związku z operacjami przetwarzania danych (analogiczna regulacja z 6 miesięcznym terminem funkcjonuje obecnie, w art. 32 ust. 5 ustawy o ochronie danych osobowych).

Jedynym ograniczeniem wskazanym w art. 98b tych obowiązków będzie niepoinformowanie podmiotu danych o zautomatyzowanych decyzjach i profilowaniu oraz ich konsekwencjach, gdyż w przypadku działań ustawowych UFG takie konsekwencje mogłoby zawierać w sobie m.in. wykrywanie przestępstw.

Dla celów antyfraudowych, dla jakich UFG przetwarza, w interesie całego sektora ubezpieczeniowego dane osobowe (m.in. poprzez prowadzenie Bazy Danych Ubezpieczonych, o której mowa w art. 102a ustawy o UFG), niewątpliwe ograniczenie praw podmiotów danych jest zasadne w oparciu o przesłanki wskazane w art. 23 ust 1 lit. d oraz e rozporządzenia 2016/679, tj. w celu wykrywania lub ścigania czynów zabronionych oraz z uwagi na ważny interes gospodarczy lub finansowy Unii lub państwa członkowskiego.

W przypadku ograniczenia praw wskazanych w art. 12 i 34 rozporządzenia dla innych celów przetwarzania danych należy wskazać, iż UFG jest instytucją powołaną przede wszystkim do wykonywania określonych zadań publicznych, wobec których cel i zakres przetwarzania danych są wyraźnie opisane w przepisach ustawy o UFG. Dodatkowo, Fundusz jest zasilany środkami podmiotów sektora ubezpieczeniowego, które wypełniają obowiązki wobec podmiotów danych z art. 12, 13 i 34 rozporządzenia 2016/679. Zatem podmiot danych ma pełną możliwość skorzystania m.in. z prawa dostępu do treści danych u samego ubezpieczyciela, zapoznania się z konsekwencjami profilowania i zostanie powiadomiony

w przypadku naruszeń bezpieczeństwa danych. Nałożenie analogicznych, nieograniczonych obowiązków na UFG powoduje podwójne obciążenie dla sektora ubezpieczeniowego, z którego UFG czerpie informacje. Podmioty tego sektora musiałyby wypełniać wspomniane obowiązku de facto podwójnie, we własnym imieniu i za pośrednictwem UFG. Ponadto, jak wspomniano wcześniej, nie jest to niezbędne z uwagi na fakt, iż działalność UFG jest w większości szczegółowo opisana w przepisach powszechnie obowiązującego prawa, zatem konsumenci mogą w każdej chwili zapoznać się podstawowymi zasadami działania Funduszu.

Należy przy tym pamiętać, iż sam art. 12 rozporządzenia 2016/679 w ust. 5 zezwala na pobierania opłaty od podmiotu danych w określonych przypadkach. Niemniej, z uwagi na fakt, iż Fundusz wykonuje zadania publiczne, zasadne jest doprecyzowanie i potwierdzenie takiej możliwości wprost w przepisach krajowych.

Wreszcie należy zauważyć, iż UFG nie jest instytucją nastawioną na zysk, głównym celem jej utworzenie jest obsługa sektora ubezpieczeniowego. Z uwagi na ilość informacji przetwarzanych przez Fundusz, spełnienie obowiązku prowadzenia korespondencji z podmiotami danych oraz obowiązku notyfikacji w przypadku naruszenia ochrony danych osobowych, wymagałoby znacznego zwiększenia środków potrzebnych na utrzymanie Funduszu, a w początkowym okresie mogłoby prowadzić do sparaliżowania jego prac. Niewątpliwe w przypadku UFG, które zajmuje się w znacznym stopniu przetwarzaniem danych, można powiedzieć, iż spełnienie obowiązków wskazanych w art. 12 i 34 rozporządzenia 2016/679 wymagałoby niewspółmiernie dużego wysiłku. Z uwagi na kluczową dla bezpieczeństwa sektora ubezpieczeniowego rolę UFG, także nałożenie na Fundusz nadmiernego obowiązku należy uznać niezasadne z uwagi na przesłanki wskazane w art. 23 ust 1 lit. d oraz e rozporządzenia 2016/679.

Odnośnie propozycji art. 98c - w zakresie pełnienia przez UFG funkcji ośrodka informacji i prowadzenia Bazy Danych Ubezpieczonych (art. 102 i 102a ustawy o UFG), które to działania Fundusz podejmuje m.in. w celu weryfikacji i przeciwdziałania naruszeniu interesów uczestników rynku ubezpieczeniowego należy podkreślić, iż jednymi z najskuteczniejszych metod przeciwdziałania oszustwom jest automatyczne przetwarzanie dużych ilości danych i szukanie korelacji wskazujących na możliwość wystąpienia niepożądanego zachowania.

Przetwarzanie i wymiana danych, o której stanowią powyższe przepisy pozwala na zapobieganie przestępstwom popełnianym na szkodę instytucji ubezpieczeniowych i jej klientów. Z uwagi na fakt, iż zadania wskazane w art. 102 i 102a ustawy o UFG należą do zadań publicznych a profilowanie stanowi szczególny rodzaj operacji wykonywanych na danych osobowych zasadne jest doprecyzowanie w samej ustawie, iż UFG jest uprawnione do wykonywania tego typu operacji. Należy przy tym podkreślić, iż przepisy rozporządzenia 2016/679 w żaden sposób nie zabraniają profilowania podmiotów danych przez Fundusz, z uwagi jednak na fakt, iż przetwarzanie danych dla celów wskazanych w art. 102 i 102a ustawy o UFG odbywać się będzie w oparciu o przesłankę art. 6 ust. 1 lit. c rozporządzenia 2016/679 (przetwarzanie danych w celu wypełnienia ciążącego na administratorze obowiązku prawnego), proponowany przepis art. 98c ma jedynie na celu doprecyzowanie, iż ramach tych zdań Fundusz będzie uprawniony także profilowania dla tych celów. Ma również na celu rozwianie wątpliwości czy podmiot danych ma prawo sprzeciwu, o którym mowa w art. 21 rozporządzenia 2016/679.

System wymiany danych wykorzystujący analizy opierające się na profilowaniu niewątpliwie może przyczynić się do ograniczania ryzyka operacyjnego występującego w podmiotach działających w sektorze ubezpieczeniowym oraz do zmniejszenia strat wynikających z przestępstw popełnianych na ich szkodę oraz szkodę ich klientów. Należy podkreślić, iż analogiczne operacje wykorzystywane są z dużym powodzeniem dla ochrony sektora bankowego.

W przypadku zaś podejmowania zautomatyzowanych decyzji w przypadku przetwarzania danych dla celów wskazanych w art. 88 i 98 ustawy o UFG, tj. dla likwidacji szkód i egzekucji należności na rzecz UFG oraz podejmowania zautomatyzowanych decyzji w przypadku przetwarzania danych dla celu prowadzenia Bazy Danych Ubezpieczonych należy podkreślić, iż jako zautomatyzowane decyzje należy uznać takie operacje przetwarzania, które wywołują skutki prawne dla podmiotu danych. Wynik przetwarzania danych przez UFG wskazuje, że operacje przetwarzania danych niewątpliwe będą wywoływały skutki prawne dla podmiotów danych.

Z drugiej strony, automatyczne podejmowanie takich decyzji w oparciu m.in. o profilowanie prowadzi do minimalizacji ryzyka wystąpienia błędów.

Jak wspomniano wcześniej, z uwagi na publicznoprawny charakter tych zadań zasadne jest, aby możliwość podejmowania automatycznych decyzji była wskazana w przepisach wprost a w konsekwencji wyłączone byłoby prawo do niepodlegania takim decyzjom.

Celem dodania art. 98d jest jedynie doprecyzowanie, iż Fundusz jest uprawniony do dalszego powierzenia przetwarzania danych. Z uwagi na publicznoprawny charakter zadań wykonywanych przez Fundusz taka możliwość, dopuszczalna w ramach przepisów rozporządzenia 2016/679, powinna znaleźć się, dla uniknięcia wątpliwości, w przepisach ustawy o UFG.

Propozycja zmian art. 102 ust. 7 i art. 102a ust. 1 jest uzasadniona koniecznością doprecyzowania w ustawie, w odniesieniu do celu przetwarzanych danych osobowych, wszystkich zadań Funduszu.

Zmiana art. 122 ust. 1 i dodanie ust. 3 - Polskie Biuro Ubezpieczycieli Komunikacyjnych („PBUK” lub „Biuro”) wykonuje zadania wynikające z ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (dalej „ustawa”), przede wszystkim w zakresie likwidacji szkód oraz pośredniczenie w wymianie informacji na temat wypadków drogowych (art. 122 ustawy). Propozycja zmiany ma na celu jednoznaczne wskazanie wykonywanych przez Biuro zadań ustawowych.

Celem dodania ust. 3 w art. 122 ustawy jest doprecyzowanie, iż PBUK jest uprawnione do dalszego powierzenia przetwarzania danych. Z uwagi na publicznoprawny charakter zadań wykonywanych przez Biuro taka możliwość, dopuszczalna w ramach przepisów rozporządzenia 2016/679, powinna znaleźć się, dla uniknięcia wątpliwości, w przepisach ustawy.

Propozycja dodania art. 136a – mając na uwadze fakt, iż PBUK wykonuje zadania wynikające z przepisów ustawy, dodanie powyższych przepisów ma na celu jednoznacznie wskazanie podstawy prawnej oraz celu przetwarzania danych w związku z wykonywaniem przez Biuro zadań ustawowych.

Przepisy ustawy nakładają na PBUK obowiązki, z którymi wiąże się konieczność przetwarzania danych osobowych. Przepis art. 6 ust. 1 rozporządzenia 2016/679 określa podstawy prawne przetwarzania danych osobowych, wśród nich - w lit. c - przesłankę stanowiącą, że administrator jest zobowiązany do przetwarzania danych w celu wypełnienia

ciążącego na nim obowiązku prawnego. Jednocześnie, art. 6 ust. 3 rozporządzenia 2016/679 nakazuje, aby przesłanka obowiązku prawnego była wyraźnie określona w prawie państwa członkowskiego. Przepisy lokalne powinny także określać co najmniej cel takiego przetwarzania. Proponowana modyfikacja jest zatem uzasadniona ze względu na konieczność wyraźnego wskazania obowiązków jakie ciążą na Biurze, a w związku z którymi konieczne jest przetwarzanie danych osobowych oraz konieczność doprecyzowanie celów przetwarzania danych w związku z wykonywaniem przez Biuro wymienionych zadań.

Ponadto, PBUK przetwarza szczególne kategorie danych, opisane w art. 9 ust. 1 oraz art. 10 rozporządzenia 2016/679 tj. dane dotyczące stanu zdrowia, a także dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa. W przypadku tych danych należy osobno wskazać, jakie przepisy ustawy stanowić będą podstawę ich przetwarzania. Nie wszystkie bowiem zadania Biura wymagają przetwarzania szczególnych kategorii danych, natomiast możliwość ich wykorzystania przez Biuro musi być wskazana wprost.

Zatem propozycja dodania art. 136a jest uzasadniona ze względu na konieczność doprecyzowania regulacji ustawowej w odniesieniu do zakresu i celu przetwarzanych szczególnych kategorii danych osobowych w celu wykonywania przez Biuro jego zadań ustawowych.

Zgodnie z art. 10 rozporządzenia 2016/679, przetwarzanie danych o wyrokach skazujących powinno mieć nie tylko wyraźną podstawę w przepisach prawa, ale również dodatkowo zabezpieczone, jeżeli chodzi o prawa i wolności podmiotów danych. Takim zabezpieczeniem będzie ograniczenie kategorii odbiorców danych osobowych.

W zakresie propozycji dodania art. 136b i 136c wskazać należy, że art. 23 rozporządzenia 2016/679 dopuszcza możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i 34, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym m.in. 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.

W zakresie ograniczenia prawa wskazanego w art. 12, 13 i 14 rozporządzenia 2016/679, dotyczącego przejrzystej i „wszelkiej" komunikacji z podmiotem danych oraz przekazania podstawowych informacji na temat procesów przetwarzania danych, należy na wstępie zauważyć, iż motyw 62 preambuły rozporządzenia 2016/679 wyraźnie wskazuje, iż ograniczenie obowiązków informacyjnych wobec podmiotów danych jest w szczególności możliwe wtedy, kiedy przetwarzanie danych ma miejsce na podstawie przepisów prawa, podmiot danych dysponuje informacjami dotyczącymi szczegółów operacji przetwarzania danych lub wykonanie obowiązku wobec podmiotów danych wymagałoby niewspółmiernie dużego wysiłku.

W motywie tym podkreśla się, że „sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności w przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia."

Z kolei motyw 63 stwierdza, że „każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (…)."

Należy zauważyć, iż wymienione w motywie 62 przesłanki nie muszą być spełnione łącznie, jednak w przypadku PBUK niewątpliwe możliwe jest wykazanie większości okoliczności zwalniających z konieczności wykonywania wspomnianych obowiązków.

Należy jednocześnie wyjaśnić, iż celem proponowanych przepisów art. 136c nie jest wyłączenie obowiązku wskazania podstawowych informacji na temat przetwarzania danych, o których mowa w art. 14 rozporządzenia 2016/679, a jedynie ich ograniczenie, szczególnie w przypadkach międzynarodowej wymiany danych, z uwagi niewspółmiernie duże obciążenie dla PBUK, jakie powodowałby obowiązek każdorazowego przekazywania informacji na temat procesów przetwarzania danych przez PBUK.

Ponadto, należy podkreślić, iż PBUK przetwarza dane w celu wykonywania określonych zadań publicznych, wobec których cel i zakres przetwarzania danych są wyraźnie opisane w przepisach ustawy.

Jak już wspomniano wcześniej, wypełnianie przez PBUK wskazanych wyżej obowiązków częściej nie jest niezbędne z uwagi na fakt, iż działalność PBUK jest szczegółowo opisana w przepisach powszechnie obowiązującego prawa, zatem konsumenci mogą w każdej chwili zapoznać się podstawowymi zasadami działania Biura.

Ograniczenie wykonywania uprawnienia wskazanego w art. 12 i 15 rozporządzenia 2016/679 ma na celu jedynie ograniczenie możliwości korzystania w szczególności z prawa dostarczenia dodatkowych wyjaśnień w związku z operacjami przetwarzania danych i prawa dostępu do danych w taki sposób, by PBUK było w stanie faktycznie wykonywać ten obowiązek (analogiczna regulacja z 6 miesięcznym terminem funkcjonuje obecnie, w art. 32 ust. 5 ustawy o ochronie danych osobowych). Biuro jest instytucją niewielką pod względem organizacyjnym i nie posiada obecnie możliwości wypełniania częściej obowiązków wskazanych w art. 12 i 15 rozporządzenia 2016/679.

Dodatkowo należy podnieść, że Biuro jest zasilane środkami finansowymi podmiotów sektora ubezpieczeniowego, które wypełniają obowiązki wobec podmiotów danych z art. 12, 13, 14, 15, 19 i 34 rozporządzenia 2016/679. Zatem podmiot danych ma pełną możliwość skorzystania m.in. z prawa dostępu do treści danych u samego ubezpieczyciela. Nałożenie analogicznych, nieograniczonych obowiązków na PBUK powoduje podwójne obciążenie dla sektora ubezpieczeniowego, z którego PBUK czerpie informacje i środki na działalność. Podmioty tego sektora musiałyby wypełniać wspomniane obowiązku de facto podwójnie, we własnym imieniu i za pośrednictwem PBUK.

W przypadku ograniczenia stosowania art. 12 rozporządzenia 2016/679 należy również podkreślić, iż sam ten przepis w ust. 5 zezwala na pobieranie opłaty od podmiotu danych w określonych przypadkach. Z uwagi na fakt, iż Biuro wykonuje zadania publiczne, zasadne jest doprecyzowanie i potwierdzenie takiej możliwości wprost w przepisach niniejszej ustawy.

Zgodnie z proponowanym art. 136c pkt 3 i 4, ograniczeniu podlegałoby również spełnienie obowiązków wskazanych w art. 19 i 34 rozporządzenia 2016/679. W przypadku art. 19 ograniczenie to jest uzasadnione nadmiernym kosztem realizacji obowiązku po stronie PBUK, w przypadku art. 34 obowiązek mógłby zostać ograniczony, o ile jego realizacja spowodowałaby nadmierny koszt po stronie PBUK. Należy podkreślić, iż środki PBUK są ograniczone, a ich przeznaczeniem jest likwidacja szkód. Waga tych zadań powoduje, iż

nałożenie na Biuro nadmiernych obciążeń finansowych należy uznać za niezasadne z uwagi na przesłankę wskazaną w art. 23 ust 1 lit. e rozporządzenia 2016/679.

W zakresie propozycji dodania art. 136d wskazać należny, że w przypadku działań publicznych wykonywanych przez Biuro w zakresie likwidowania szkód przez PBUK (art. art. 122 ust. 1 pkt 3 i 4 i art. 123 pkt 1 i 2 ustawy), które to działania PBUK podejmuje w interesie poszkodowanych należy podkreślić, iż jedną z najskuteczniejszych metod reagowania na zdarzenia drogowe oraz konieczność likwidacji szkód byłoby, związane z tymi procesami, automatyczne przetwarzanie informacji i podejmowanie zautomatyzowanych decyzji.

Z uwagi na fakt, iż zadania wskazane w powyższych przepisach ustawy należą do zadań publicznych, a zautomatyzowane podejmowanie decyzji stanowi szczególny rodzaj operacji wykonywanych na danych osobowych zasadne jest doprecyzowanie w samej ustawie, iż PBUK jest uprawnione do wykonywania tego typu operacji. Należy przy tym podkreślić, iż przepisy rozporządzenia 2016/679 w żaden sposób nie zabraniają podejmowania zautomatyzowanych decyzji przez PBUK. Jednak z uwagi na fakt., iż przetwarzanie danych dla celów wskazanych w art. art. 122 ust. 1 pkt 3 i 4 i art. 123 pkt 1 i 2 ustawy odbywać się będzie w oparciu o przesłankę art. 6 ust. 1 lit. c RODO (przetwarzanie danych w celu wypełnienia ciążącego na administratorze obowiązku prawnego), proponowany przepis art. 136e ma jedynie na celu doprecyzowanie, iż w ramach tych zadań Biuro będzie uprawnione także do podejmowania zautomatyzowanych decyzji dla tych celów. Ma również na celu rozwianie wątpliwości czy podmiot danych ma prawo do niepodlegania takim decyzjom, o którym mowa w art. 22 ust. 2 rozporządzenia 2016/679.

Za zautomatyzowane decyzje należy uznać takie operacje przetwarzania, które wywołują skutki prawne dla podmiotu danych. Wynik przetwarzania danych przez PBUK wskazuje, że operacje przetwarzania danych niewątpliwie będą wywoływały skutki prawne dla podmiotów danych.

Propozycja dodania art. 136e i art. 136f - wprowadzenie tych regulacji ma charakter doprecyzowujący i porządkujący. PBUK jest instytucją uprawnioną do przetwarzania, na podstawie przepisów prawa, danych o szczególnym charakterze, wskazanych w art. 9 i art. 10 RODO, tj. danych na temat stanu zdrowia oraz dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Zgodnie z art. 10 rozporządzenia 2016/679, przetwarzanie danych o wyrokach skazujących powinno mieć nie tylko wyraźną podstawę w przepisach prawa, ale również powinno być dodatkowo zabezpieczone w odniesieniu do praw i wolności podmiotów danych. Takim zabezpieczeniem będzie wyraźne ustalenie w przepisach ustawy katalogu podmiotów uprawnionych do otrzymywania danych od PBUK.

Natomiast proponowany okres retencji jest dostosowany do okresu przedawnienia roszczeń wobec Biura w związku z wykonywaniem zadań wskazanych w art. 123 oraz wykonaniem obowiązków wynikających z art. 133 i art. 134 ustawy.

50. Ustawa z dnia 13 czerwca 2003 r. o zatrudnieniu socjalnym

Zmiany w ustawie z dnia 13 czerwca 2003 r. o zatrudnieniu socjalnym upoważniają podmioty tworzące centra integracji społecznej i kluby integracji społecznej do przetwarzania danych osobowych uczestników tych centrów i klubów. W obowiązującym stanie prawnym brak jest przepisu upoważaniającego do przetwarzania danych osobowych tych osób, a ze względu na fakt, że część tych danych to dane szczególnie chronione, niezbędne jest nadanie upoważnienia w akcie rangi ustawowej. Nakłada się również ustawowy obowiązek zachowania poufności wszelkich informacji i danych, które podmioty i osoby wykonujące zadania w ramach centrów i klubów integracji społecznej uzyskały przy wykonywaniu tych zadań.

Z uwagi na treść art. 23 ust. 1 lit. e rozporządzenia 2016/679, który umożliwia przyjęcie przez Państwo członkowskie ograniczeń zakresu obowiązków i praw przewidzianych w niektórych przepisach ww. rozporządzenia m in. w dziedzinie zabezpieczenia społecznego, projekt ustawy wyłącza w stosunku do przetwarzania danych osobowych uczestników centrów i klubów integracji społecznej, następujące obowiązki:

- informowania uczestników centrów i klubów integracji społecznej w przypadku zbierania danych pochodzących od tych osób (art. 13 rozporządzenia 2016/679),

- informowania uczestników centrów i klubów integracji społecznej w przypadku pozyskania danych ich dotyczących od innych podmiotów (art. 14 rozporządzenia 2016/679),

- prawa dostępu do przetwarzanych danych osobowych (art. 15 rozporządzenia 2016/679),

- prawa do ograniczenia przetwarzania danych osobowych (art. 18 rozporządzenia 2016/679),

- powiadamianie o sprostowaniu, usunięciu, ograniczeniu przetwarzania danych osobowych (art. 19 rozporządzenia 2016/679),

- prawo do sprzeciwu wobec przetwarzania danych osobowych (art. 21 rozporządzenia 2016/679).

Realizując wymóg określony w art. 23 ust. 2 rozporządzenia 2016/679 wprowadza się w art. 8b ust. 3 – 7 oraz art. 18d ust. 3- 7 ustawy o zatrudnieniu socjalnym przepisy dotyczące celu przetwarzania danych osobowych, zakresu wprowadzanych ograniczeń, wskazania administratora danych, zabezpieczenia danych osobowych oraz okresu przechowywania danych.

Jako administratora danych osobowych uczestników centrum integracji społecznej wskazuje się to centrum, gdyż centrum przetwarza dane osobowe jako jednostka organizacyjna utworzona przez jednostkę samorządu terytorialnego w formie jednostki budżetowej lub samorządowego zakładu budżetowego, przez organizację pozarządową lub przez podmioty, o których mowa w art. 3 ust. 3 pkt 1 i 3 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz. U. z 2016 r. poz. 1817 i 1948 oraz z 2017 r. poz. 60 i 573). Jako administratorów danych osobowych uczestników klubów integracji społecznej wskazano podmioty, które je utworzyły.

Projekt nakłada obowiązek zabezpieczenia danych osobowych uczestników centrów i klubów integracji społecznej przed nadużyciami i niezgodnym z prawem dostępem lub przekazywaniem, poprzez zastosowanie procedur prawnych, w których toku dane są przetwarzane.

Okres przechowywania danych osobowych będzie ustalał administrator zgodnie z celami ich przetwarzania.

51. Ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami

Zaproponowane zmiany w art. 8 ust. 1a, art. 14a ust. 1a, art. 22 ust. 7, art. 23 ust. 3, art. 24a ust. 1a, art. 25 ust. 3, art. 27 ust. 2, art. 29 ust. 4a, art. 30 ust. 2a, art. 32 ust. 11, art. 34 ust. 2b, art. 35a, art. 36 ust. 9, art. 38 ust. 1c, art. 50a, art. 59a ust. 3, art. 58a, art. 74 ust. 3, art. 81 ust. 3, art. 82a ust. 3, art. 83 ust. 2, art. 83a ust. 2a, art. 90 ust. 3, art. 91 ust. 5, art. 98 ust. 2a, art. 99a, art. 101a, art. 105a oraz art. 106 ust. 5 ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opieki nad zabytkami (Dz. U. z 2014 r. poz. 1446, z późń. zm.) mają na celu ustalenie katalogów danych osobowych przetwarzanych przez organy państwowe odpowiedzialne za ochronę zabytków. Propozycje czynią z jednej strony zadość wymogom

konstytucyjnym, aby ograniczenia praw i wolności wynikały bezpośrednio z ustawy, z drugiej - wymaganiom art. 6 ust. 1 lit. c rozporządzenia 2016/679, który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego, wojewódzcy konserwatorzy zabytków i Generalny Konserwator Zabytków oraz pozostałe podmioty jako podmioty publiczne narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Prawa określone w art. 13 i 14 rozporządzenia 2016/679 (prawo do informacji) także miałyby być ograniczone w ten sposób, że nie znalazłyby one zastosowania w zakresie, w jakim dane te są niezbędne do zapewnienia prawidłowej realizacji zadań, obowiązków i uprawnień.

Prawo do sprostowania danych byłoby wyłączone w przypadkach zbierania danych w celu prowadzenia dokumentacji aukcji, których przedmiotem są zabytki archeologiczne albo przedmioty wykopane z ziemi o cechach zabytku.

Prawo do ograniczenia przetwarzania danych, obowiązek informowania o sprostowaniu danych oraz prawo do przenoszenia danych byłyby wyłączone w przypadkach przetwarzania danych, o których mowa w art. 8 ust. 1, art. 14a ust. 1a, art. 22 ust. 7, art. 23 ust. 3, art. 24a ust. 1a, art. 34 ust. 2b, art. 59a ust. 3, art. 101 ust. 1a i art. 105a ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opieki nad zabytkami.

Z kolei obowiązku poinformowania podmiotu, którego dane dotyczą, o naruszeniu ochrony danych osobowych nie stosuje się, jeśli administrator w terminie 72 godzin od stwierdzenia takiego naruszenia wyda o nim komunikat na swojej stronie podmiotowej Biuletynu Informacji Publicznej lub na swojej stronie internetowej.

Wprowadzono także możliwość zlecenia innym podmiotom przez podmioty przetwarzające dane osobowe w celach związanych z ochroną zabytków przetwarzania danych

osobowych na ich rzecz oraz pełnienia przez nie funkcji przetwarzającego dane na zlecenie innego podmiotu.

Art. 23 ust. 2 rozporządzenia 2016/679 zawiera wymagania dotyczące ograniczania praw podmiotów danych. Zostały one spełnione w art. 6a ust. 1 przez określenie środków zabezpieczenia danych, okresu przechowywania danych oraz w art. 6a ust. 8 przez wskazanie sposobu ogłaszania ograniczeń praw podmiotu danych. Dodatkowo, spełniony został wymóg podania kategorii danych przez wskazanie ich zakresu w art. 8 ust. 1a, art. 14a ust. 1a, art. 22 ust. 7, art. 23 ust. 3, art. 24a ust. 1a, art. 25 ust. 3, art. 27 ust. 2, art. 29 ust. 4a, art. 30 ust. 2a, art. 32 ust. 11, art. 34 ust. 2b, art. 35a, art. 36 ust. 9, art. 38 ust. 1c, art. 50a, art. 59a ust. 3, art. 58a, art. 74 ust. 3, art. 81 ust. 3, art. 82a ust. 3, art. 83 ust. 2, art. 83a ust. 2a, art. 90 ust. 3, art. 91 ust. 5, art. 98 ust. 2a, art. 99a, art. 101a, art. 105a oraz art. 106 ust. 5 ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opieki nad zabytkami.

52. Ustawa z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego

W proponowanej zmianie przepisu art. 43 ustawy z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego (Dz. U. z 2016 r. poz. 198, 1609 i 1985 oraz z 2017 r. poz. 730 i 949), zwanej dalej „ustawą”, uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, zgodnie z którym przepis prawa krajowego powinien określać obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań ustawowych.

W związku z powyższym, w art. 43 ustawy zaproponowano zmianę polegającą na określeniu zakresu danych przetwarzanych w związku z przyznawaniem przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego dotacji na zadania objęte mecenatem państwa w dziedzinie kultury.

Proponuje się także, aby minister właściwy do spraw kultury i ochrony dziedzictwa narodowego mógł pełnić funkcję podmiotu przetwarzającego dane osobowe lub zlecać przetwarzanie w swoim imieniu danych osobowych podmiotowi przetwarzającemu.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister jako podmiot publiczny narażony byłby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, poprzez wprowadzenie normy nakazującej nie później niż 72 godziny od stwierdzenia naruszenia, umieszczenie przez administratora danych osobowych komunikatu na stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej.

Prawa określone w art. 13 oraz art. 14 rozporządzenia 2016/679 (prawo do informacji) również byłyby ograniczone.

Należy podkreślić, że administrator byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

53. Ustawa z dnia 28 listopada 2003 r. o świadczeniach rodzinnych

Zmiana o charakterze czysto technicznym polegająca na usunięciu odesłania w art. 23 ust. 9 do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

54. Ustawa z dnia 12 marca 2004 r. o pomocy społecznej

Zmiany do ustawy z dnia 12 marca 2004 r. o pomocy społecznej upoważniają podmioty, którym zlecono realizację zadania z zakresu pomocy społecznej, do przetwarzania, na zasadach określonych w przepisach o ochronie danych osobowych, danych osobowych w zakresie niezbędnym do realizacji zleconego zadania. W obowiązującym stanie prawnym brak jest przepisu upoważaniającego do przetwarzania danych osobowych przez podmioty realizujące zadania pomocy społecznej na zlecenie jednostek samorządu terytorialnego. Nakłada się również ustawowy obowiązek zachowania poufności wszelkich informacji i danych, które podmioty i osoby wykonujące zadania zlecone do realizacji uzyskały przy wykonywaniu tych zadań.

Z uwagi na treść art. 23 ust. 1 lit. e rozporządzenia 2016/679, który umożliwia przyjęcie przez Państwo członkowskie ograniczeń zakresu obowiązków i praw przewidzianych w niektórych przepisach ww. rozporządzenia m in. w dziedzinie zabezpieczenia społecznego, projekt ustawy wyłącza w stosunku do przetwarzania danych osobowych osób ubiegających się i korzystających ze świadczeń pomocy społecznej, następujące obowiązki:

- informowania osób ubiegających się i korzystających ze świadczeń pomocy społecznej w przypadku zbierania danych pochodzących od tych osób (art. 13 rozporządzenia 2016/679),

- informowania ww. osób w przypadku pozyskania danych ich dotyczących od innych podmiotów (art. 14 rozporządzenia 2016/679),

- prawa dostępu do przetwarzanych danych osobowych (art. 15 rozporządzenia 2016/679),

- prawa do ograniczenia przetwarzania danych osobowych (art. 18 rozporządzenia 2016/679),

- powiadamianie o sprostowaniu, usunięciu, ograniczeniu przetwarzania danych osobowych (art. 19 rozporządzenia 2016/679),

- prawo do sprzeciwu wobec przetwarzania danych osobowych (art. 21 rozporządzenia 2016/679).

Wyłączenie będzie miało zastosowanie w przypadku danych osobowych niezbędnych do przyznawania, udzielania i kontroli świadczeń z pomocy społecznej.

Realizując wymóg określony w art. 23 ust. 2 rozporządzenia 2016/6 wprowadza się w art. 100 ust. 4 – 7 ustawy o pomocy społecznej przepisy dotyczące celu przetwarzania danych osobowych, zakresu wprowadzanych ograniczeń, wskazania administratora danych, zabezpieczenia danych osobowych oraz okresu przechowywania danych.

Jako administratorów danych osobowych przetwarzanych w celu przyznawania i udzielania świadczeń z pomocy społecznej projekt wskazuje publiczne jednostki organizacyjne wykonujące zadania w zakresie pomocy społecznej.

Projekt nakłada obowiązek zabezpieczenia danych osobowych osób ubiegających się i korzystających ze świadczeń pomocy społecznej przed nadużyciami i niezgodnym z prawem dostępem lub przekazywaniem, poprzez zastosowanie procedur prawnych, w których toku dane są przetwarzane.

Okres przechowywania danych osobowych będzie ustalał administrator zgodnie z celami ich przetwarzania.

Art. 126 ustawy o pomocy społecznej uzupełnia się o upoważnienie wojewodów wykonujących zadania w ramach kontroli i nadzoru w pomocy społecznej do przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli.

55. Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarzadzaniu alternatywnymi funduszami inwestycyjnymi

Dokonywana zmiana ma charakter ma charakter porządkowy. Obowiązujące przepisy w zakresie ochrony danych osobowych - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) zostanie uchylona. Odwołania zawarte w ustawie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych musiały więc zostać dostosowane do nowej sytuacji prawnej. Ponieważ zasady przekazywania danych do państwa trzeciego nie będą już określane w przepisach krajowych postanowiono odesłać w tym zakresie do regulacji zawartych w rozporządzeniu 2016/679.

56. Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej

Propozycje w zakresie art. 34 wynikają z konieczności zachowania zgodności przepisów z zasadami celowości i proporcjonalności przetwarzania danych osobowych oraz prawem do bycia zapomnianym. Na aspekt ten zwrócił uwagę GIODO komentując identyczne przepisy zawarte w nowym projekcie ustawy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej oraz Punkcie Informacji dla Przedsiębiorcy (CEIDGPiP). GIODO zasugerował wskazanie okresu, przez jaki dane przedsiębiorcy będą przechowywane w CEIDG po wykreśleniu jego wpisu z ewidencji. Zgadzając się z argumentami GIODO zaproponowano wskazanie 10-cio letniego okresu przetwarzania danych przedsiębiorcy wykreślonego z CEIDG. Tak wskazany okres realizuje wyżej wskazane zasady przetwarzania danych osobowych przedsiębiorców wykreślonych z CEIDG, którego celem jest umożliwienie ustalenia zmian zachodzących we wpisach przedsiębiorcy, np. w celu dochodzenia roszczeń od tego przedsiębiorcy.

Propozycja w zakresie art. 39b uzasadniona jest tym, że w momencie wejścia w życie rozporządzenia 2016/679, ustawa wskazana w art. 39b ustawy o swobodzie działalności gospodarczej, czyli dotychczasowa ustawa o ochronie danych osobowych, przestanie obowiązywać. Tym niemniej, należy zauważyć, że uchylany przepis jest korzystny dla przedsiębiorców przetwarzających dane osobowe innych przedsiębiorców wpisanych

do CEIDG (przedsiębiorca posiadający bazę swoich kontrahentów - wpisanych jednocześnie do CEIDG - np. na potrzeby fakturowania, nie miał obowiązku zgłaszania tej bazy do GIODO).

57. Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne

Zmiana w zakresie treści art. 174:

ustawa z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, 1579, 1823, 1948, 1954, 2003, z 2017 r. poz. 935), zwana dalej „ustawą – PT", w zakresie sposobu wyrażenia zgody, o której mowa w art. 174 stanowi implementację dyrektywy 2002/58 (zob. art. 2 lit. f). Natomiast rozporządzenie 2016/679 - stosownie do art. 95 - „nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie 2002/58/WE".

Zgodnie z motywem 17 dyrektywy 2002/58 „Do celów niniejszej dyrektywy, zgoda użytkownika lub abonenta, niezależnie od tego czy abonentem jest osoba fizyczna czy prawna, powinna mieć to samo znaczenie co zgoda podmiotu danych opisana i szerzej określona w dyrektywie 95/46/WE. Zgoda może być udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, włączając zaznaczenie okna wyboru podczas przeglądania witryny internetowej". Przepisy dyrektywy 2002/58 odwołują się do konstrukcji zgody zawartej w przepisach o ochronie danych osobowych.

W kontekście powyższego należy zwrócić uwagę, iż zgodnie z treścią art. 94 ust. 1 rozporządzenia 2016/679: „Dyrektywa 95/46/WE zostaje uchylona ze skutkiem od dnia 25 maja 2018 r."). W związku z tym należy w ramach treści art. 174 pr. tel. odwołać się do treści przepisów o ochronie danych, w tym rozporządzenia 2016/679 (definicja zgody zamieszczona w art. 174 ustawy – PT, powinna uwzględnić zmianę kontekstu systemowego podobnie jak w przypadku uśude). W konsekwencji zmiany wymaga obecny 174 ustawy – PT. Należy zwrócić uwagę, iż projektodawca nie zdecydował się zmienić art. 173 ustawy - PT. W związku z tym kryteria skutecznej zgody, o których mowa w art. 174 ustawy - PT dookreślane są m.in. w art. 173 ust. 2 ustawy – PT.

Uchylenie art. 174a-174d prawa telekomunikacyjnego:

uchylenie art. 174a-174d jest konsekwencją treści przepisów Rozporządzenia 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej.

Zmiany w art. 159 i 161 prawa telekomunikacyjnego:

przepisy rozdziału VII ustawy - PT w obecnym kształcie - zawierają regulacje dotyczące przetwarzania danych dotyczących użytkownika będącego osobą fizyczną, które nie stanowią implementacji dyrektywy 2002/58. Dane te nie są objęte treścią art. 95 rozporządzenia 2016/679, w związku z czym należy je wyłączyć spod regulacji ustawy - PT i objąć przepisami o ochronie danych osobowych. Odnosi się to do danych dotyczących użytkowników będących osobami fizycznymi innych wskazane w art. 159 ust. 1 pkt 2-5 ustawy - PT. Oznacza to, iż objęte regulacją ustawy prawo telekomunikacyjne pozostaje przetwarzanie danych wskazanych w art. 159 ust. 1 lit. 2-5 także w zakresie w jakim dotyczą one osób fizycznych i mogą być kwalifikowane jako dane osobowe w rozumieniu przepisów rozporządzenia 2016/679.

Co istotne, w zakresie nieuregulowanym przepisami prawa telekomunikacyjnego (także w odniesieniu do danych wskazanych w art. 159 ust. 1 lit. 2-5 ustawy - PT) do przetwarzania danych osobowych zastosowanie znajdą przepisy o ochronie danych osobowych, w tym regulacja rozporządzenia 2016/679.

W pozostałym zakresie zmiany w ustawie prawo telekomunikacyjne mają charakter porządkujący.

58. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych

W projektowanej zmianie zawartej w pkt 1 rozwiązywany jest dotychczasowy problem braku formalnego uregulowania kto jest administratorem danych osobowych określonych w art. 32b ust. 4 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2016 r., poz. 1793, z późn. zm.), zwanej dalej „ustawą ośoz”, tj. danych osobowych zawartych w Karcie Diagnostyki i Leczenia Onkologicznego (dalej zwanej „Kartą DILO”). Wydaje się być naturalne, iż w sytuacji, gdy Karta DILO zawierająca dane osobowe w rozumieniu RODO, pozostaje u świadczeniodawcy (co oznacza, że ten gromadzi dane osobowe, a zatem dokonuje czynności wyczerpującej znamiona przetwarzania tego typu

danych), świadczeniodawca ten powinien być uznany za administratora danych osobowych, i jako taki wskazany wprost w przepisie prawa.

Przepis dotyczący zawartości Karty DILO stanowi sam w sobie unormowanie dające podstawę, by w odniesieniu do niego określić, kto jest administratorem danych osobowych. Niemniej jednak należy mieć na względzie, że zgodnie z dyspozycją przepisu art. 32b ust. 3 ustawy ośoz Kartę DILO, w przypadkach, o których mowa w art. 32a ust. 2 tej samej ustawy, pozostawia się u lekarza POZ i dołącza się ją do dokumentacji medycznej, z czego wynika, że istnieją przypadki, kiedy Karta staje się elementem tej dokumentacji.

W tym też kontekście, kwestię uregulowania kto jest administratorem danych osobowych zawartych w Karcie DILO, można by potraktować jako składową uregulowania dotyczącego szerszego problemu, tj. przetwarzania danych osobowych gromadzonych (a zatem – przetwarzanych) w dokumentacji medycznej, co można potraktować jako możliwe podejście alternatywne w stosunku do opcji rozbudowywania art. 32b ustawy ośoz o kwestie przetwarzania danych osobowych.

Niezależnie od powyższego, wskazuje się, że biorąc pod uwagę przepisy rozporządzania2016/679, jednym z działań koniecznych do przeprowadzenia w poszczególnych krajowych przepisach (w tym tych dot. ochrony zdrowia) jest wyraźne określenie kto stanowi administratora danych osobowych w przypadkach, gdy dane takie są na podstawie tychże przepisów przetwarzane (w celach innych niż cele osobiste, domowe lub innych przypadkach przetwarzanie wyłączonych spod stosowania rozporządzenia 2016/679). Działań takich nie sposób jest skutecznie przeprowadzić w sposób inny niż ingerencja legislacyjna.

Projektowana zmiana wprowadza także do ustawy ośoz przepisy pozwalające Narodowemu Funduszowi Zdrowia, zwanemu dalej „NFZ” na nieinformowanie osób, których dane NFZ pozyskał w związku ze zgłoszeniem do ubezpieczenia zdrowotnego i opłacaniem składek (m.in. od świadczeniodawców udzielających świadczeń opieki zdrowotnej, ZUS, czy KRUS) o każdym przypadku przetwarzania danych, jeśli przetwarzane dane osobowe były pozyskane od podmiotów innych niż osoby, których te dane dotyczą. Zwolnienie z obowiązku informowania osób, których dane NFZ przetwarza, jest możliwe o ile przepisy prawa krajowego wydane na podstawie na art. 23 rozporządzenia 2016/679 rozwiązanie takie przewidują, a przetwarzanie danych (informacji) jest związane z interesem publicznym w obszarze zdrowia publicznego i zabezpieczenia społecznego.

W przypadku realizacji obowiązku informacyjnego minimum raz w miesiącu i informowania o każdorazowym przetwarzaniu danych osobowych, NFZ poniósłby znaczne koszty, a z uwagi na liczbę osób, których dane są przez Fundusz przetwarzane – realizacja obowiązku byłaby niewykonalna.

Przyjęcie proponowanego rozwiązania spowoduje zaoszczędzenie znacznych kwot, ponieważ cena listu poleconego w obrocie krajowym z usługą zwrotne potwierdzenie odbioru zgodnie z umową na usługi pocztowe zawartą przez Centralę NFZ i Pocztą Polską S.A. na 2017 r. o wadze do 50 g wynosi 6,20 zł, to w przypadku 300 milinów listów rocznie ponieważ przekazywane dane byłyby najczęściej danymi wrażliwymi wynosiłaby 1, 860 mln zł. Natomiast koszty kopert druku, papieru - ponad 30 mln zł. Do powyższych kwot należałoby jeszcze dołożyć koszty obsługi, koszty zatrudnienia dodatkowych osób obsługujących ww. proces co wydaje się niewykonalne w ramach przyznanych NFZ środków na wynagrodzenia oraz koszt wprowadzenia niezbędnych zmian informatycznych. Dodatkowo należałoby założyć co najmniej dwa lata na wprowadzenie niezbędnych zmian w systemach informatycznych.

W pozostałych zmianach wprowadzanych w ustawie uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679, zgodnie z którym przepis prawa krajowego powinien określać obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań ustawowych.

59. Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych

Zmiana ma charakter dostosowawczy i związana jest ze zmianą organu właściwego w sprawach ochrony danych osobowych

60. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

Zmiany o charakterze technicznym polegające na usunięciu odesłania do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

61. Ustawa z dnia 30 czerwca 2005 r. o kinematografii

W projektowanych zmianach ustawy z dnia 30 czerwca 2005 r. o kinematografii (Dz. U z 2016 r. poz. 438 oraz z 2017 r. poz. 961) uwzględniono brzmienie art. 6 ust. 1 lit. c

rozporządzenia 2016/679, który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych. Zagadnienie to uregulowano w nowym Rozdziale 4a, w art. 30a- 30b.

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.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego, Polski Instytut Sztuki Filmowej, Filmoteka Narodowa oraz filmoteki regionalne jako podmioty publiczne finansowane ze środków publicznych, w tym niektóre z dotacji udzielanych z budżetów odpowiednio: państwa lub jednostki samorządu terytorialnego, narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony danych, na podstawie art. 34 rozporządzenia 2016/679, wprowadzając zarazem normę nakazującą umieścić na stronie podmiotowej Biuletynu Informacji Publicznej informację o zaistniałym naruszeniu w terminie 72 godzin od stwierdzenia naruszenia.

Prawo określone w 14 rozporządzenia 2016/679 (prawo do informacji, w przypadku pozyskania danych nie od osoby, której dotyczą), zostały wyłączone z uwagi na fakt, iż nie jest możliwe do spełnienia w przypadku przetwarzania danych do celów wskazanych w art. 28 ust. 2 pkt 3, 5 i 6, tj.:

- gromadzenie i archiwizacja dokumentacji dotyczącej produkcji filmów i rozpowszechniania filmów;
- gromadzenie zbiorów bibliotecznych oraz eksponatów dotyczących historii filmu i kinematografii;
- prowadzenie katalogu dzieł filmowych.

Jednocześnie nakłada się obowiązek zamieszczenia na stronie podmiotowej w Biuletynie Informacji Publicznej, stosownej informacji o obowiązujących ograniczeniach i włączeniach.

Tak jak w wypadku przetwarzania danych do innych celów związanych z dofinansowaniem

działalności kulturalnej, proponowany okres retencji danych przetwarzanych w celu dofinansowywania przedsięwzięć z zakresu przygotowania projektów filmowych, produkcji filmów, dystrybucji filmów i rozpowszechniania filmów, promocji polskiej twórczości filmowej i upowszechniania kultury filmowej, w tym produkcji filmów podejmowanych przez środowiska polonijne oraz związanych z tym usług eksperckich wynosi 20 lat.

62. Ustawa z dnia ustawie z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym

Zmiana o charakterze porządkowym. Uchylona zostanie regulacja zgodnie z którą zbiór danych osobowych, osób korzystających z systemu biblioteczno-informacyjnego, jest zwolniony z obowiązku rejestracji zbiorów danych osobowych, o których mowa w art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Uchylenie tego przepisu zapewni zgodność regulacji zawartej w art. 88 ustawy – Prawo o szkolnictwie wyższym z rozporządzeniem 2016/679, które nie przewiduje obowiązku rejestracji zbiorów danych. Ponadto należało uchylić odesłanie do uchylanej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

63. Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii

Zmiana o charakterze technicznym polegająca na usunięciu odesłania do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

64. Ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych

Dokumenty paszportowe są jednym z dwóch rodzajów dokumentów, które potwierdzają tożsamość obywateli polskich umożliwiając przede wszystkim przekraczanie granic. Dokument ten daje rękojmię prawdziwości zawartych w nim danych nie tylko polskim organom ale przede wszystkim organom innych państw. W związku z tym, w celu jednoznacznego przypisania określonej osoby do wydanego jej dokumentu i zapewnienie tym samym pewności obrotu prawno-administracyjnego prowadzone są ewidencje paszportowe, centralna ewidencja wydanych i unieważnionych dokumentów paszportowych oraz gromadzona jest odpowiednia dokumentacja. W związku z powyższym przetwarzanie danych osobowych na potrzeby wydawania dokumentów paszportowych jest uregulowane w sposób szczególny w już obecnie obowiązującej ustawie o dokumentach paszportowych.

Ustawa o dokumentach paszportowych nie zawierała szczegółowych regulacji dotyczących przetwarzania danych osobowych w tym zasad ich zbierania, zakresu zbieranych

danych, wskazania właściwości i zadań organów w zakresie zapewnienia bezpieczeństwa przetwarzanych danych, trybu usuwania niezgodności w zakresie gromadzonych danych, zasad dostępu do danych dla osób, których dane dotyczą czy też czasu przechowywania danych.

Dostosowanie ustawy do rozporządzenia 2016/679 polegało przede wszystkim uregulowaniu ww. kwestii oraz:

1) konieczności doprecyzowania zasad przetwarzania danych osobowych w związku z wykonywaniem zadania publicznego jakim jest wydawanie obywatelom polskim dokumentów paszportowych;
2) doprecyzowanie jakie organy i w jakim zakresie przetwarzają dane osobowe, oraz jasny podział zadań związany z przetwarzaniem danych osobowych w centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych oraz w ewidencjach paszportowych, w tym określenie właściwości poszczególnych podmiotów, tj. ministra właściwego do spraw informatyzacji, ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw zagranicznych, w zakresie zapewnienia bezpieczeństwa przetwarzania danych osobowych centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych i ewidencji paszportowych i przetwarzanych w nich danych osobowych
3) jasne wskazanie celu przetwarzania danych osobowych na potrzeby wydania obywatelowi polskiemu dokumentu paszportowego, w tym wiarygodnego powiązania osoby z wydawanym jej dokumentem paszportowym, a także ustalenia i umożliwienia ustalenia prawa do posiadania dokumentu paszportowego oraz zgodnie z art. 23 rozporządzenia Parlamentu Europejskiego i rady (UE) 2016/67 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 65/46/WE (ogólne rozporządzenie o ochronie danych) wskazano, których przepisów ww. rozporządzenia nie stosuje się w stosunku do przetwarzania danych na potrzeby realizacji zadania leżącego w ogólnym interesie publicznym oraz na potrzeby zapewnienia bezpieczeństwa publicznego;
4) szczegółowym określeniu jakiego rodzaju dane są gromadzone w centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych i w ewidencjach paszportowych, a także określeniu, iż danych zgromadzonych w ww. ewidencjach nie usuwa się, za wyjątkiem danych określonych w art. 46 ust. 4 pk4 (tj. biometrycznych w postaci odcisków palców);
5) szczegółowe określenie zasad i trybu udostępniania danych osobowych z centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych oraz z ewidencji

paszportowych na wniosek uprawnionych, ściśle określonych w ustawie podmiotów i tylko w zakresie niezbędnym do wykonywania ustawowych zadań (np. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, czy Centralnemu Biuru Antykorupcyjnemu).

W ramach przetwarzania danych osobowych na potrzeby prowadzenia spraw paszportowych, tj. związanych z wydaniem, odmową wydania i unieważnieniem dokumentu paszportowego, ze stosowania wyłączono:

1) art. 15 rozporządzenia, gdyż biorąc pod uwagę masowy charakter przetwarzania wprowadzenie wszystkich wymagań określonych art 15 wymagałaby niewspółmiernie dużego nakładu środków, aby uzyskać pełną zgodność przekazywanych informacji z wymaganiami rozporządzenia, niemniej jednak należy wskazać, że przepisy ustawy jasno wskazują zasady udzielania osobom informacji o przetwarzanych danych osobowych zatem postulat dostępu osoby do informacji o tym jakie jej dane osobowe są przetwarzane pozostaje spełniony;
2) art. 16 rozporządzenia, gdyż dane w centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych oraz w ewidencjach paszportowych muszą być referencyjne i pewne zatem niedopuszczalne jest dokonywanie sportowania danych jedynie na podstawie oświadczenia osoby, której dane dotyczą, ustawa jasno wskazuje tryb usuwania niezgodności danych zawartych w centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych lub w ewidencjach paszportowych , zatem podstawowe prawo osoby jakim jest prawo do sprostowania danych jest zachowane;
3) art. 18 rozporządzenia, gdyż musi istnieć możliwość nieprzerwanego przetwarzania danych przez organy publiczne zatem ograniczenie przetwarzania danych nie jest dopuszczalne;
4) art. 21 rozporządzenia, gdyż przetwarzane w centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych i w ewidencjach paszportowych dane są kluczowe dla ustalania tożsamości osób fizycznych zatem nie jest dopuszczalne zaprzestanie przetwarzania danych danej osoby na podstawie jej sprzeciwu.

65. Ustawa z dnia 25 sierpnia 2006 r. o biokomponentach i biopaliwach ciekłych

Pomimo, że w rejestrach, których dotyczą ww. przepisy (rejestr wytwórców oraz rejestr podmiotów sprowadzających) nie gromadzi się danych osobowych (art. 5 ust. 4 pkt 1 oraz art. 12c ust. 3 pkt 1 stanowią, że we wniosku należy ujawnić oznaczenie firmy wytwórcy, jej siedziby, adresu oraz inne dane teleadresowe) proponuje się wprowadzić projektowaną zmianę

celem zapewnienia spójności ustawy – analogiczna zmiana będzie bowiem konieczna do wprowadzenia w przypadku kolejnego rejestru, który dane osobowe zawiera. Ponadto, proponowana zmiana pozwoli uniknąć wątpliwości pojawiających się w związku z obecnym brzmieniem ww. przepisu czy dane podmiotu wykreślonego są nadal widoczne, ale np. z adnotacją „wykreślony" lub odpowiadającym jej oznaczeniem graficznym. W praktyce, obecnie, wykreślenie jest równoznaczne z fizycznym usunięciem podmiotu z rejestru.

Proponowana zmiana w art. 15 ust. 3 wynika z konieczności zapewnienia należytej ochrony danych osobowych podmiotu wpisywanego do rejestru, zgodnie z wymaganiami nałożonymi przez rozporządzenie 2016/679.

Biorąc pod uwagę jawny charakter rejestru oraz wprowadzone w art. 17 rozporządzenia 2016/679 prawo do usunięcia danych w ww. projektowanych przepisach proponuję doprecyzować kwestię skutku wykreślenia danych z rejestrów i wyraźnie określić, że wykreślenie z danego rejestru jest równoznaczne z fizycznym usunięciem z tego rejestru danych wykreślanego podmiotu. Pozwoli to uniknąć wątpliwości pojawiających się w związku z obecnym brzmieniem ww. przepisu czy dane podmiotu wykreślonego są nadal widoczne, ale np. z adnotacją „wykreślony" lub odpowiadającym jej oznaczeniem graficznym.

Jednocześnie wszystkie usuwane z rejestrów prowadzonych na podstawie przedmiotowej ustawy dane nadal znajdują się w złożonych do organu rejestrowego wnioskach o wpis do rejestru, które stanowią akta sprawy. Ponieważ organ rejestrowy – Prezes Agencji Rynku Rolnego jest organem państwowym, do postępowania z aktami sprawy stosuje przepisy ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2016 r. poz. 1506, z późn. zm.), w rozumieniu której, akta sprawy są materiałem archiwalnym podlegającym archiwizacji przez okres czasu zgodny z nadaną im kategorią, zgodnie z wewnętrzną instrukcją kancelaryjną (w Agencji Rynku Rolnego akta te maja kategorię archiwalną A). W związku z tym, zrezygnowano z wprowadzania do przedmiotowej ustawy odrębnych przepisów regulujących okres przechowywania wniosków o wpis do rejestru.

66. Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym

Zmiana o charakterze technicznym polegająca na usunięciu odesłania do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

67. Ustawa z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944 – 1990 oraz treści tych dokumentów

W związku z tym, że Generalny Inspektor Ochrony Danych Osobowych w wyniku zmian wprowadzonych ustawą o ochronie danych osobowych stanie się Prezesem Urzędu Ochrony Danych Osobowych, a Biuro Generalnego Inspektora Ochrony Danych Osobowych przekształcone zostanie w Urząd Ochrony Danych Osobowych, konieczne stało się zastąpienie w ustawie wyrazów „Generalny Inspektor Ochrony Danych Osobowych" wyrazami „Prezes Urzędu Ochrony Danych Osobowych".

68. Ustawa z dnia 12 stycznia 2007 r. o drogowych spółkach specjalnego przeznaczenia

W ustawie o drogowych spółkach specjalnego przeznaczenia dodano art. 4a, który ureguluje kwestię przetwarzania danych osobowych przez drogową spółkę specjalnego przeznaczenia. Jako, że ustawowe zadania spółki mogą być podobne do tych, które realizuje GDDKiA (m. in. pobór opłat za przejazd autostradą, pobór opłaty elektronicznej, przeciwdziałanie niszczeniu dróg przez ich użytkowników) zastosowano w zakresie przetwarzania danych przez spółkę oraz ich udostępniania uprawnionym służbom i instytucjom państwowym rozwiązania analogiczne do tych, które zaproponowano w art. 18 ust. 2a – 2j ustawy o drogach publicznych.

69. Ustawa dnia 16 lutego 2007 r. o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym

Celem zapewnienia zgodności z rozporządzeniem 2016/679 proponuje się usunąć regulację zgodnie zawartą w art. 29b ust. 5 zgodnie z którą podczas przeglądu zapasów interwencyjnych nie przetwarza się danych osobowych. Wszelkie dane zebrane podczas tego przeglądu są niezwłocznie usuwane.

70. Ustawa z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów

Zmiana o charakterze technicznym polegająca na usunięciu odesłania do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

71. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta

Podstawowym zadaniem Rzecznika Praw Pacjenta jest troska o najszerzej pojęty interes pacjentów, przede wszystkim w kontekście przestrzegania ich praw. Rzecznik w ramach swojej aktywności podejmuje działania w sferze danych osobowych pacjentów, które z racji swojej wrażliwości, podlegają szczególnej ochronie, przed dostępem dla osób nieuprawnionych. Dane o stanie zdrowia są klasyfikowane, jako dane wrażliwe. Dotyczą one jednej z najbardziej intymnych sfer życia jednostki, co potwierdzi Trybunał Konstytucyjny w wyroku z dnia 19 maja 1998 r. Realizacja przez Rzecznika Praw Pacjenta swoich ustawowych kompetencji i obowiązków, wyszczególnionych w art. 47 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta zwana dalej „u.p.p., związania jest z przetwarzaniem przez ten organ danych osobowych pacjentów. Każda czynność związana z przetwarzaniem danych sensytywnych, powinna odbywać się z poszanowaniem zasad wynikających z powszechnie obowiązujących przepisów prawa. Natomiast niewłaściwe przetwarzanie danych o stanie zdrowia może doprowadzić do naruszeń praw i wolności jednostki. Na Rzeczniku Praw Pacjenta, jako administratorze danych osobowych, spoczywa ciężar dochowania szczególnej staranności w celu ochrony interesów pacjentów, przez zapewnienie, aby dane były przetwarzane zgodnie z prawem.

Prawo dostępu do danych osobowych o statusie powinno wprost wynikać z przepisów rangi ustawy. Rzecznik Praw Pacjenta dla skutecznej realizacji swoich ustawowych zadań, powinien mieć zagwarantowany szeroki dostęp do danych medycznych pacjentów, w tym także danych pozyskanych przez Rzeczników Praw Pacjenta Szpitali Psychiatrycznych, będących pracownikami Biura Rzecznika Praw Pacjenta.

Jednakże w aktualnym stanie prawnym ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta, jak również ustawa o ochronie zdrowia psychicznego nie przewiduje wprost podstawy prawnej w przedmiocie przetwarzania danych osobowych pacjentów, co jest niezbędne dla prawidłowego i skutecznego wykonywania zadań Rzecznika.

Proponowane zmiany w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta wprowadzają wyraźną podstawę prawną do przetwarzania danych osobowych pacjentów przez Rzecznika Praw Pacjenta oraz jego pracowników. Rzecznik uzyska ustawowe prawo do przetwarzania danych wrażliwych dla realizacji swoich obowiązków. Natomiast pracownicy

Biura, w tym Rzecznicy Praw Pacjenta Szpitali Psychiatrycznych, do ich gromadzenia i przekazywania dla potrzeb wykonywanych zadań.

72. Ustawa z dnia 21 listopada 2008 r. o służbie cywilnej

Zmiana o charakterze technicznym polegająca na usunięciu odesłania do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

73. Ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

74. Ustawa z dnia 2 kwietnia 2009 r. o obywatelstwie polskim

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

75. Ustawa z dnia 7 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

76. Ustawa z dnia 27 września 2009 r. o finansach publicznych

Zmiana w art. 139 ust. 2 ma charakter dostosowawczy i związana jest ze zmianą organu właściwego w sprawach ochrony danych osobowych.

77. Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych

Zmiana art. 9f ust. 1 pkt 8 ma charakter dostosowujący i związana jest ze zmianą organu właściwego w sprawach ochrony danych osobowych.

Dodawany art. 16b przewiduje odpowiednie stosowanie przepisów art. 13c, art. 106d, art. 112b ust. 1 i art. 112e Prawa bankowego, które zostały szczegółowo omówione w uzasadnieniu do zmian Prawa Bankowego.

78. Ustawa z dnia 19 listopada 2009 r. o grach hazardowych

W proponowanej zmianie przepisu art. 87 ustawy z dnia 19 listopada 2009 r. o grach hazardowych uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679, zgodnie z którym przepis prawa krajowego powinien określać obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań ustawowych.

W związku z powyższym w przepisach ustawy zaproponowano zmiany polegające na określeniu zakresu danych przetwarzanych w związku z przyznawaniem przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego nagród, stypendiów oraz prowadzonych programów.

Jednocześnie proponuje się wyraźne wskazanie okresów przechowywania danych osobowych w związku z realizacją ww. celów.

Proponuje się także, aby minister właściwy do spraw kultury i ochrony dziedzictwa narodowego mógł pełnić funkcję podmiotu przetwarzającego dane osobowe lub zlecać przetwarzanie w swoim imieniu danych osobowych podmiotowi przetwarzającemu.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i art. 15 rozporządzeniem 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego dysponujący Funduszem Promocji Kultury jako podmiot publiczny narażony byłby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, przez wprowadzenie normy nakazującej nie później niż 72 godziny od stwierdzenia naruszenia, umieszczenie komunikatu na stronie podmiotowej w Biuletynie Informacji Publicznej lub na swojej stronie internetowej. Prawa określone w art. 13 (prawo do informacji) oraz art. 19 (obowiązek powiadomienia odbiorców o sprostowaniu danych) rozporządzenia 2016/679 również byłyby ograniczone.

Niewspółmiernym do kosztów prowadzonych przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego działań byłby również koszt dokumentowania realizacji zadań z zakresu ochrony danych, dlatego proponuje się ograniczenie stosowania przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego art. 5 ust. 2 rozporządzenia 2016/679. Należy podkreślić, że minister właściwy do spraw kultury i ochrony dziedzictwa narodowego byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach na stronie podmiotowej w Biuletynie Informacji Publicznej.

79. Ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych

W związku z tym, że Generalny Inspektor Ochrony Danych Osobowych w wyniku zmian wprowadzonych ustawą o ochronie danych osobowych stanie się Prezesem Urzędu Ochrony Danych Osobowych, a Biuro Generalnego Inspektora Ochrony Danych Osobowych przekształcone zostanie w Urząd Ochrony Danych Osobowych, konieczne stało się zastąpienie w ustawie z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, wyrazów „Generalny Inspektor Ochrony Danych Osobowych" wyrazami „Prezes Urzędu Ochrony Danych Osobowych".

80. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

Zmiana o charakterze porządkowym. W związku z tym, że Generalny Inspektor Ochrony Danych Osobowych w wyniku zmian wprowadzonych ustawą o ochronie danych osobowych stanie się Prezesem Urzędu Ochrony Danych Osobowych, a Biuro Generalnego Inspektora Ochrony Danych Osobowych przekształcone zostanie w Urząd Ochrony Danych Osobowych, konieczne stało się zastąpienie w ustawie wyrazów „Generalny Inspektor Ochrony Danych Osobowych" wyrazami „Prezes Urzędu Ochrony Danych Osobowych".

81. Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych

Dowód osobisty jest jednym z dwóch rodzajów dokumentów, który potwierdza tożsamość obywatela polskiego. W celu jednoznacznego przypisania określonej osoby do wydanego jej dokumentu i zapewnienie tym samym pewności obrotu prawno-administracyjnego prowadzony jest Rejestr Dowodów Osobistych oraz gromadzona jest odpowiednia dokumentacja. W związku z powyższym przetwarzanie danych osobowych na

potrzeby wydawania, wymiany i unieważniania dowodów osobistych jest już obecnie jasno uregulowane w ustawie o dowodach osobistych.

Z uwagi na to, że zmieniana ustawa o dowodach osobistych zawiera wiele bardzo szczegółowych regulacji dotyczących przetwarzania danych osobowych, w tym zasady ich zbierania, zakres zbieranych danych, wskazuje również właściwe organy i ich zadania a także zasady dostępu do danych zarówno dla osób, których dane dotyczą, jak i dla innych osób fizycznych oraz pozostałych podmiotów, dostosowanie ustawy do rozporządzenia 2016/679 polegało przede wszystkim na:

1. konieczności doprecyzowania zasad przetwarzania danych osobowych w związku z wykonywaniem zadania publicznego jakim jest wydawanie, wymiana i unieważnianie dowodów osobistych;
2. doprecyzowanie w jakim zakresie uprawnione organy przetwarzają dane osobowe,
3. określenie okresu przetwarzania danych;
4. doprecyzowanie procedury w przypadku stwierdzenia niezgodności danych zawartych we wniosku z danymi zawartymi w Rejestrze Dowodów Osobistych;
5. określenie zasad sprostowania i uzupełnienia danych dotyczących wniosku o wydanie dowodu osobistego;
6. jasne wskazanie celu przetwarzania danych osobowych, tj. w interesie publicznym oraz w celu zapewnienia bezpieczeństwa publicznego poprzez zapewnienie bezpieczeństwa obrotu prawnego dokumentami tożsamości wydawanym obywatelom polskim, w tym wiarygodnego powiązania osoby z wydawanym dowodem osobistym oraz umożliwienia wydawania obywatelom polskim dokumentów tożsamości oraz zgodnie z art. 23 rozporządzenia 2016/67 wskazano, których przepisów ww. rozporządzenia nie stosuje się w stosunku do przetwarzania danych na potrzeby wydawania, wymiany i unieważniania dowodów osobistych.

W ramach przetwarzania danych osobowych na potrzeby wydawania, wymiany i unieważniania dowodów osobistych oraz prowadzenia Rejestru Dowodów Osobistych ze stosowania wyłączono:

1) art. 15 rozporządzenia, gdyż biorąc pod uwagę masowy charakter przetwarzania wprowadzenie wszystkich wymagań określonych art 15 wymagałaby niewspółmiernie dużego nakładu środków aby uzyskać pełną zgodność przekazywanych z wymaganiami rozporządzenia, niemniej jednak należy wskazać, że przepisy ustawy jasno wskazują zasady

udzielania osobom informacji o przetwarzanych danych osobowych zatem postulat dostępu osoby do informacji o tym jakie jej dane osobowe są przetwarzane pozostaje spełniony;
2) art. 16 rozporządzenia , gdyż dane w Rejestrze Dowodów Osobistych muszą być referencyjne i pewne, zatem niedopuszczalne jest dokonywanie sprostowania danych jedynie na podstawie oświadczenia osoby, której dane dotyczą, projektowane zmiany w ustawie o dowodach osobistych. jasno wskazują tryb prostowania danych w rejestrze , zatem podstawowe prawo osoby jakim jest prawo do sprostowania danych jest zachowane;
3) art. 18 rozporządzenia, gdyż musi istnieć możliwość nieprzerwanego przetwarzania danych przez organy publiczne, zatem ograniczenie przetwarzania danych jest niedopuszczalne,
4) art. 21 rozporządzenia, gdyż przetwarzane w rejestrze dane są kluczowe dla ustalania tożsamości osób fizycznych, zatem nie jest dopuszczalne zaprzestanie przetwarzania danych danej osoby na podstawie jej sprzeciwu.

82. Ustawa z dnia 24 września 2010 r. o ewidencji ludności

Prowadzenie ewidencji ludności i nadawanie osobom numeru PESEL służy utrzymaniu i rozwojowi, podstawowej bazy danych osobowych- rejestru PESEL- umożliwiającej jednoznaczną identyfikację osób fizycznych, zawierającą przede wszystkim ich aktualne dane. Rejestr PESEL jest rejestrem referencyjnym dla wielu innych rejestrów państwowych. W związku z powyższym dane w tym rejestrze muszą być kompletne, aktualne i zgodne ze stanem faktycznym i prawnym, a dostęp do rejestru jednoznacznie określony, co już obecnie jest jasno uregulowane w ustawie o ewidencji ludności.

Mając na względzie, że zmieniana ustawa o ewidencji ludności zawiera wiele szczegółowych regulacji dotyczących przetwarzania danych osobowych, w tym zasady ich zbierania, zakres zbieranych danych, wskazuje właściwe organy i ich zadania, tryby zmiany, uzupełniania i sprostowania danych, zasady dostępu do danych zarówno dla osób, których dane dotyczą, jak i dla innych osób fizycznych oraz pozostałych podmiotów czy też zasady przechowywania danych,

Dostosowanie ustawy do rozporządzenia 2016/679 polegało przede wszystkim na:

1) konieczności doprecyzowania zasad przetwarzania danych osobowych w związku z wykonywaniem zadania publicznego prowadzenie ewidencji ludności polegającej na rejestracji

określonych w ustawie podstawowych danych identyfikujących tożsamość oraz status administracyjnoprawny osób fizycznych,

2) doprecyzowanie zakresu, w jakim uprawnione organy przetwarzają dane osobowe,

3) określenie okresu przetwarzania danych osobowych

4) sprecyzowanie celu przetwarzania danych osobowych, tj. w interesie publicznym oraz w celu zapewnienie bezpieczeństwa publicznego poprzez zapewnienie jednoznacznej identyfikacji oraz ustalenia statusu administracyjno-prawnego osób fizycznych oraz zgodnie z art. 23 rozporządzenia 2016/67 wskazano, których przepisów ww. rozporządzenia nie stosuje się w stosunku do przetwarzania danych na potrzeby prowadzenie ewidencji ludności.

W ramach przetwarzania danych osobowych na potrzeby prowadzenia ewidencji ludności, w tym prowadzenia rejestru PESEL, ze stosowania wyłączono:

1) art. 15 rozporządzenia, gdyż biorąc pod uwagę masowy charakter przetwarzania wprowadzenie wszystkich wymagań określonych art. 15 wymagałaby niewspółmiernie dużego nakładu środków aby uzyskać pełną zgodność przekazywanych z wymaganiami rozporządzenia, niemniej jednak należy wskazać, że przepisy ustawy jasno wskazują zasady udzielania osobom informacji o przetwarzanych danych osobowych, zatem postulat dostępu osoby do informacji o tym, jakie jej dane osobowe są przetwarzane pozostaje spełniony;

2) art. 16 rozporządzenia, gdyż dane w rejestrze PESEL muszą być referencyjne i pewne, zatem niedopuszczalne jest dokonywanie sprostowania danych, jedynie na podstawie oświadczenia osoby, której dane dotyczą, ustawa o ewidencji ludności jasno wskazuje tryb prostowania danych w rejestrze, zatem podstawowe prawo osoby jakim jest prawo do sprostowania danych jest zachowane;

3) art. 18 rozporządzenia, gdyż musi istnieć możliwość nieprzerwanego przetwarzania danych przez organy publiczne, zatem ograniczenie przetwarzania danych nie jest dopuszczalne;

4) art. 21 rozporządzenia, gdyż przetwarzane w rejestrze dane są kluczowe dla ustalania tożsamości osób fizycznych zatem niedopuszczalne jest zaprzestanie przetwarzania danych danej osoby na podstawie jej sprzeciwu.

83. Ustawa z dnia 5 stycznia 2011 r. - Kodeks wyborczy

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

84. Zmiany w ustawie z dnia 25 marca 2011 r. o Centrum Polsko - Rosyjskiego Dialogu i Porozumienia

W projektowanych przepisach ustawy z dnia 25 marca 2011 r. o Centrum Polsko-Rosyjskiego Dialogu i Porozumienia (Dz. U. z 2016 r. poz. 494) uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679, który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych przetwarzanych w ramach poszczególnych zadań ustawowych. W związku z powyższym w projekcie zaproponowano zmiany określające zarówno zakres danych przetwarzanych w związku z przyznaniem przez Centrum Polsko-Rosyjskiego Dialogu i Porozumienia stypendiów i dofinansowania. Z tego samego powodu proponuje się wprowadzenie nowego art. 27a określającego obowiązek przetwarzania danych w związku z wykonywaniem przez ministra właściwego do spraw kultury i dziedzictwa narodowego oraz Centrum określonych w ustawie zadań.

Wprowadzono także możliwość zlecenia innym podmiotom przez ministra właściwego do spraw kultury i dziedzictwa narodowego oraz Centrum przetwarzania danych na swoją rzecz oraz pełnienia przez ministra właściwego do spraw kultury i dziedzictwa narodowego oraz Centrum funkcji przetwarzającego dane na zlecenie innego podmiotu.
Jednocześnie proponuje się wskazanie 20-letniego okresu przechowywania danych osobowych w związku z realizacją zadań, o których mowa w art. 24-25. W pozostałym zakresie okres przetwarzania danych byłby zależny od realizacji celu przetwarzania.

W związku z koniecznością przetwarzania danych o skazaniach, wprowadza się zakaz ich udostępniania innym podmiotom jako dodatkową gwarancję, o której mowa w art. 10 rozporządzenia 2016/679.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym

państwa: minister właściwy do spraw kultury i dziedzictwa narodowego oraz Centrum jako podmioty publiczne narażone byłoby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponujemy ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, poprzez wprowadzenie normy nakazującej nie później niż 72 godziny od stwierdzenia naruszenia, umieszczenie komunikatu na stronie podmiotowej w Biuletynie Informacji Publicznej. Prawa określone w art. 13 rozporządzenia 2016/679 (prawo do informacji) oraz 19 rozporządzenia 2016/679 (obowiązek poinformowania o sprostowaniu danych) również byłyby ograniczone w takim zakresie, w jakim są niezbędne do realizacji zadań ustawowych administratora danych osobowych. Należy podkreślić, że administrator byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach poprzez umieszczenie stosownej informacji na stronie BIP.

85. Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej

W proponowanych zmianach ustawy zgodnie z propozycją ministra właściwego do spraw kultury i dziedzictwa narodowego, uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań.

Z tego względu proponuje się wprowadzenie do ustawy przepisów określających obowiązki przetwarzania danych w związku z wykonywaniem określonych w tych ustawach zadań.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego w zakresie, w jakim sprawuje nadzór nad szkolnictwem artystycznym, inne jednostki nadzoru nad tym szkolnictwem, szkoły i placówki artystyczne jako podmioty publiczne narażone byłyby na

poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, zobowiązując zarazem administratora danych do umieszczenia na swojej stronie internetowej lub w Biuletynie Informacji Publicznej komunikatu o zaistniałym naruszeniu nie później niż 72 godziny od stwierdzenia naruszenia. Wprowadzenie ograniczeń praw określonych w art. 13 i 14 (prawo do informacji) oraz obowiązku, o którym mowa w art. 5 ust. 2 rozporządzenia 2016/679 (dokumentowanie przestrzegania przepisów o ochronie danych) jest konieczne nie tylko z uwagi na nadmierny koszt ale również inne niewspółmierne nakłady.

Należy podkreślić, że administrator byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach i włączeniach na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

86. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej

W zmianach wprowadzanych w ustawie uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia 2016/679, zgodnie z którym przepis prawa krajowego powinien określać obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań ustawowych.

87. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia

Celem zaproponowanych zmian jest dostosowanie obowiązujących przepisów ustawy o systemie informacji w ochronie zdrowia do regulacji rozporządzenia 2016/679.

Proponowane zmiany w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2016 r. poz. 1535, z późn. zm.) dotyczą przede wszystkim przepisów dotyczących ochrony danych osobowych. W art. 19 w ust. 1 ustawy dodano pkt 4, w którym wskazano nowy cel przetwarzania danych w rejestrach medycznych poprzez odniesienie do badań naukowych i statystycznych, co jest spójne z ust. 7 art. 19 ustawy, w którym przewidziano możliwość przetwarzania danych osobowych w postaci ich udostępniania z rejestrów medycznych w celu prowadzenia badań naukowych i do celów statystycznych wyłącznie po ich anonimizacji. W przywołanym ust. 7 ujednolicono terminologię z rozporządzeniem 2016/679 poprzez zastąpienie pojęcia „cele naukowo-badawcze” na „w celu prowadzenia badań naukowych”.

Zaproponowano także usunięcie obowiązku informacyjnego nałożonego na podmiot prowadzący rejestr medyczny w stosunku do osób, których dane dotyczą i są przetwarzane w rejestrze. W myśl bowiem art. 14 ust. 5 lit. b RODO, obowiązek informacyjny administratora danych osobowych nie ma zastosowania, jeżeli udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile ten obowiązek może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. Podmioty prowadzące rejestry medyczne, tj. podmioty lecznicze, w których niejednokrotnie znajduje się dziesiątki tysięcy i więcej danych osobowych, nie mają fizycznej możliwości poinformowania osób, których dane są przetwarzane w rejestrze, o przetwarzaniu w tych rejestrach danych dotyczących pacjentów. Nie dysponują bowiem aktualnymi danymi adresowymi pacjentów, a koszty tej operacji, przy bazach danych zawierających nawet kilkaset tysięcy pacjentów byłyby nieproporcjonalne w stosunku do przewidywanych korzyści. Zasadnym jest zatem zrezygnowanie z tego obowiązku, poprzez usunięcie całego ust. 9, w szczególności, że przedmiotowa problematyka została kompleksowo uregulowana w rozporządzeniu 2016/679.

Ponadto, usunięto z przepisów odniesienia do minimalnych norm technicznych zabezpieczania przetwarzania danych osobowych, w szczególności przetwarzanych w systemach teleinformatycznych, z uwagi na odmienne rozwiązanie przyjęte w rozporządzeniu 2016/679. W świetle art. 32 rozporządzenia 2016/679 oraz zasady neutralności technologicznej, to że systemy w których przetwarzane są dane osobowe mają być bezpieczne jest zadaniem administratora, który sam decyduje o środkach jakie podejmie by zapewnić to bezpieczeństwo, przepisy prawa tych kwestii nie powinny regulować. Dotychczas ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia w dwóch jednostkach redakcyjnych wymaga, aby gromadzone dane podlegały ochronie na poziomie wysokim, o którym mowa w przepisach wydanych na podstawie art. 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (art. 9a ust. 2 oraz art. 20 ust. 6), w związku z powyższym należało usunąć te regulacje.

88. Ustawa z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej

Propozycja zmian dotycząca ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej polega na zmianie w art. 7 w ust. 2 odwołania do art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Obecnie obowiązujące przepisy odwołują się do art. 25 ust 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Obecne przepisy ustawy o wspieraniu rodziny i systemie pieczy zastępczej w sposób niebudzący wątpliwości wskazują zakres i cel przetwarzania danych osobowych. Jednocześnie należy zaznaczyć, iż nie ma możliwości enumeratywnego wskazania katalogu osób czy też spraw, do którego przedmiotowy zakres ustawy miałby zastosowanie. Specyfika spraw, w których zastosowanie znajdują przepisy o przetwarzaniu danych osobowych w zakresie realizacji ustawy o wspieraniu rodziny i systemie pieczy zastępczej uwzględnia obowiązek zachowania w tajemnicy informacji o osobach, do których stosuje się tę ustawę, oraz członków ich rodzin, w tym informacji o udzielonych tym osobom pomocy i świadczeniach, co znajduje wyraz w art. 7 ust. 3 ustawy.

89. Ustawa z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących

Zmiana o charakterze porządkowym.

90. Ustawa z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych

Wprowadzenie zmiany w ustawie z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych (Dz. U. poz. 1038, z późn. zm.) jest zmianą o charakterze doprecyzowującym i porządkowym, która jednoznaczne wskazuje, podmiot odpowiedzialny za administrację danych osobowych zawartych w rejestrze pielęgniarek i położnych prowadzonym przez okręgowe rady pielęgniarek i położnych

Zmiana spowodowana jest wejściem w życie rozporządzenia 2016/679. Powstała konieczność jednoznacznego wskazania podmiotu odpowiedzialnego za administracje danych osobowych zawartych w rejestrach pielęgniarek i położnych, o których mowa w art. 31 pkt 3 ustawy z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych - jako administratora tych danych wskazano – Okręgowe Rady Pielęgniarek i Położnych.

91. Ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej

W związku z wejściem w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) powstaje konieczność jednoznacznego wskazania podmiotu odpowiedzialnego za administracje danych osobowych zawartych w Centralnym Rejestrze Pielęgniarek i Położnych, o którym mowa w art. 43 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2016 r. poz. 1251, z późn. zm.) poprzez zmianę wskazującą, jako administratora tych danych – Naczelną Radę Pielęgniarek i Położnych.

92. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych

Zmiana w art. 10 ust. 1 ma charakter dostosowujący i polega na zmianie odesłania do przepisu rozporządzenia 2016/679.

Dodanie art. 10 ust. 2:

W związku z faktem, iż biometria stanowi coraz istotniejszą kwestię w świadczeniu usług płatniczych, w szczególności w zakresie tzw. silnej weryfikacji uwierzytelniania klienta, konieczne jest wprowadzenie w ustawie o usługach płatniczych odpowiedniej podstawy prawnej uprawniającej niebankowych dostawców usług płatniczych, t.j. instytucje płatnicze (IP), instytucje pieniądza elektronicznego (IPP), do przetwarzania tych danych. Silne uwierzytelnianie klienta ma zapewniać wyższy poziom wiarygodności i odporności na oszustwa w związku z realizacją płatności elektronicznych i oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających. W związku z faktem, iż dane biometryczne wchodzą w skład elementów w oparciu o które można dokonywać uwierzytelniania na potrzeby realizacji transakcji płatniczych należy dokonać przedmiotowej zmiany art. 10 ustawy.

Dodany art. 10a stanowi podstawę prawną do przetwarzania danych o niekaralności pracowników instytucji płatniczych oraz instytucji pieniądza elektronicznego. Ponadto art. 10 a tworzy podstawę prawną do przetwarzania przez instytucje płatnicze i instytucje pieniądza elektronicznego jako pracodawców określonych danych biometrycznych swoich pracowników, celem monitorowania dostępu do pomieszczeń i informacji tych instytucji. W wielu sytuacjach dostęp do poszczególnych danych bądź fizycznych pomieszczeń – w szczególności tych najbardziej poufnych - uzależniony jest od skanowania odcisków palców bądź rogówki oka. Dodatkowo, potrzeba taka istniałaby w przypadku pracowników posiadających dostęp do gotówki.

Dodanie art. 10b:

Rozporządzenie 2016/679 daje możliwość ograniczenia obowiązków administratora i przetwarzającego, wynikających z art. 12-22 oraz 34 i 5rozporzadzenia 2016/679, o ile zakłada to prawo UE bądź państwa członkowskiego. Przepis art. 23 ust. 1 określa, jakie cele ma realizować taki przepis ograniczający obowiązki.

W przypadku sektora usług płatniczych, na uwagę zasługują przede wszystkim środki służące:

- zapewnieniu bezpieczeństwu publicznego (lit. c),

- przeciwdziałaniu przestępczości, (…) w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom (lit. d);

- innym ważnym celom (…) w tym kwestiom pieniężnym, budżetowym i podatkowym (…) (lit. e),

- ochronie osoby, której dane dotyczą, lub praw i wolności innych osób (lit. i).

Obowiązki administratora podlegające ograniczeniu bądź wyłączeniu dotyczą obowiązków informacyjnych, obowiązków wykonania prawa do bycia zapomnianym czy prawa do przenoszalności danych, ale także obowiązku notyfikacji naruszenia bezpieczeństwa danych wobec podmiotów danych osobowych.

Zaproponowane w art. 10b ograniczenia obowiązków nałożonych na administratorów, które powinny przysługiwać instytucją płatniczym i instytucjom pieniądza elektronicznego, polegają na:

- wyłączeniu prawa do dostępu do danych oraz prawa do informacji w zakresie obowiązków ustawowych IP i IPE dotyczących działań przeciwko oszustwom i praniu pieniędzy,

- ograniczeniu katalogu sytuacji, w których IP, IPE są obowiązane dokonywać notyfikacji naruszenia bezpieczeństwa danych wobec podmiotów, których dane dotyczą (art. 34 rozporzadzenia 2016/679) – w przypadku gdy takowa notyfikacja mogłaby spowodować naruszenie stabilności funkcjonowania IP, IPE jako instytucji finansowej,

- ograniczeniu prawa do przenoszalności danych oraz prawa do bycia zapomnianym, jeśli obowiązek dalszego przechowywania i przetwarzania danych osobowych przez IP, IPE jest niezbędny z uwagi na obowiązki ustawowe ciążące na banku.

- wyłączeniu obowiązku z art. 13 ust. 2 lit. f, art. 14 ust. 2 lit. g i art. 15 ust. 1 lit. h rozporządzenia 2016/679 w przypadku zautomatyzowanego podejmowania decyzji, w tym profilowania.

93. Ustawa z dnia 23 listopada 2012 r. – Prawo pocztowe

Zmiana wskazana w pkt 1 dotyczy przekazania wniosku o wpis do rejestru operatorów pocztowych. Wraz z wnioskiem o wpis do rejestru wyrażana będzie zgoda na przetwarzanie danych osobowych podanych we wniosku w zakresie i celu niezbędnym dla realizacji zadań i obowiązków Prezesa UKE jako organu regulacyjnego w dziedzinie rynku usług pocztowych. Jednocześnie wskazano, że wniosek może zostać złożony w postaci elektronicznej.

Zmiana wskazana w pkt 2 ma na celu określenie maksymalnego czasu przechowywania danych osobowych przez Prezesa UKE. Wprawdzie dane osobowe operatora są wykreślane z rejestru operatorów pocztowych z chwilą zaprzestania działalności pocztowej, ale ich przechowanie jest istotne, np. ze względu na obowiązki sprawozdawcze nałożone na podmiot wykreślony z rejestru, ale wykonujący działalność pocztową, w którym nastąpiło wykreślenie (art. 43 ust. 5).

94. Ustawa z dnia 14 grudnia 2012 r. o odpadach

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

95. Ustawa z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności

W związku z wejściem w życie rozporządzenia 2016/679 powstaje konieczność jednoznacznego wskazania podmiotu odpowiedzialnego za administracje danych osobowych zawartych w centralnym systemie informatycznym, poprzez wyraźne wskazanie jako administratora tych danych – ministra właściwego do spraw rozwoju regionalnego.

96. Ustawa z dnia 29 sierpnia 2014 r. o charakterystyce energetycznej budynków

Wprowadzana zmiana ma cel doprecyzowujący. Jej istotą jest wskazanie na rolę ujętego w nim podmiotu jako na administratora danych.

97. Ustawa z dnia 28 listopada 2014 r. - Prawo o aktach stanu cywilnego

Rejestracja stanu cywilnego polega na odnotowywaniu w centralnym rejestrze podstawowych zdarzeń w życiu człowieka, które kształtują byt administracyjno - prawny osoby, w tym jej podstawowe dane osobowe, takie jak: imię, nazwisko, imiona i nazwiska rodziców, datę urodzenia małżeństwa itd. Rejestr Stanu Cywilnego jest rejestrem referencyjnym dla rejestru PESEL i w związku z tym dane w tym rejestrze muszą być pewne, oparte na właściwej dokumentacji i przechowywane przez odpowiednio długi okres, a dostęp do nich jest odpowiednio uregulowany. W związku z powyższym zasady przetwarzania danych osobowych na potrzeby rejestracji stanu cywilnego muszą być dostosowane do specyfiki tego szczególnego zadania realizowanego w interesie publicznym i dla zapewnienia bezpieczeństwa publicznego,.

Zmieniana ustawa - Prawo o aktach stanu cywilnego zawiera wiele szczegółowych regulacji dotyczących przetwarzania danych osobowych, w tym dotyczących zasad ich zbierania, zakresu zbieranych danych, właściwych organów i ich zadań, trybu zmiany, uzupełniania i sprostowania danych, zasad dostępu do danych zarówno dla osób, których dane dotyczą, jaki i organów państwowych i innych osób fizycznych czy też okresu przechowywania danych. Zatem dostosowanie ustawy do rozporządzenia 2016/679 polegało przede wszystkim na:

7. konieczności doprecyzowania, że rejestracji stanu cywilnego, w interesie publicznym oraz w celu zapewnienia bezpieczeństwa publicznego, dokonuje się w rejestrze stanu cywilnego w formie aktów stanu cywilnego dla odzwierciedlenia stanu cywilnego danej

osoby. Określenie celu przetwarzania danych jest niezbędne w świetle art. 6 ust. 3 pkt 3 rozporządzenia.

8. doprecyzowaniu, jakie organy i w jakim zakresie przetwarzają dane osobowe, oraz określeniu podziału zadań związanych z przetwarzaniem danych osobowych w rejestrze stanu cywilnego. Zaproponowane regulacje odzwierciedlają stan faktyczny w tym zakresie, niemniej w świetle rozporządzenia, niezbędnym wydaje się precyzyjne ich określenie w prawie krajowym.
9. wskazaniu, zgodnie z art. 23 rozporządzenia Parlamentu Europejskiego i rady (UE) 2016/67 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 65/46/WE (ogólne rozporządzenie o ochronie danych), których przepisów ww. rozporządzenia nie stosuje się w stosunku do przetwarzania danych na potrzeby rejestracji stanu cywilnego.

W ramach przetwarzania danych osobowych na potrzeby prowadzenia rejestracji stanu cywilnego ze stosowania wyłączono:

1) art. 15 rozporządzenia, gdyż biorąc pod uwagę masowy charakter przetwarzania wprowadzenie wszystkich wymagań określonych art 15 wymagałaby niewspółmiernie dużego nakładu środków aby uzyskać pełną zgodność przekazywanych informacji z wymaganiami rozporządzenia. Należy jednak wskazać, że przepisy PRASC jasno wskazują zasady udzielania osobom informacji o przetwarzanych danych osobowych zatem postulat dostępu osoby do informacji o tym, jakie jej dane osobowe są przetwarzane pozostaje spełniony. Dane udostępniane są w formie odpisów z aktów i zaświadczenia o zamieszczonych lub niezamieszczonych w rejestrze stanu cywilnego danych dotyczących danej osoby. W zakresie, w jakim art. 15 rozporządzenia przewidziano prawo do uzyskania informacji o kategoriach odbiorców, którym dane zostały ujawnione, w prawie krajowym przewidziano możliwość uzyskania informacji zarówno o podmiotach dokonujących operacji w rejestrze stanu cywilnego oraz możliwość uzyskania informacji o wydanych z aktu odpisach oraz o wydanych zaświadczeniach o zamieszczonych lub niezamieszczonych w rejestrze stanu cywilnego danych dotyczycących wskazanej osoby wraz z informacją komu wydano odpis lub zaświadczenie.

2) art. 16 rozporządzenia, gdyż dane w rejestrze muszą być referencyjne i pewne zatem niedopuszczalne jest dokonywanie sportowania danych jedynie na podstawie oświadczenia osoby, której dane dotyczą. Ustawa- Prawo o aktach stanu cywilnego jasno wskazuje tryb

prostowania danych w rejestrze, zatem podstawowe prawo osoby jakim jest prawo do sprostowania danych jest zachowane.
3) art. 18 rozporządzenia, gdyż musi istnieć możliwość nieprzerwanego przetwarzania danych przez organy publiczne zatem ograniczenie przetwarzania danych nie jest dopuszczalne. Ograniczenie przetwarzania danych dotyczących danej osoby w rejestrze stanu cywilnego, w przypadku, gdy osoba której dane dotyczą kwestionuje ich prawidłowość znacząco utrudniłoby funkcjonowanie takiej osoby w społeczeństwie i mogłoby się wiązać uniemożliwieniem wykonywania niektórych zadań przez organy administracji publicznej.
4) art. 21 rozporządzenia, gdyż przetwarzane w rejestrze dane są kluczowe dla ustalania tożsamości osób fizycznych zatem niedopuszczalne jest zaprzestanie przetwarzania danych danej osoby na podstawie jej sprzeciwu. Realizacja takiego prawa również oznaczałaby, że osoba nie funkcjonuje w obrocie prawnym.

Dodatkowo wprowadza się zmiany wzmacniające uprawnienia osób, których dane dotyczą, polegające na:
- wprowadzeniu uprawnienia dla osoby, której dane dotyczą, uzyskania informacji, czy udostępniono dokumenty z akt zbiorowych stanu cywilnego aktu jej dotyczącego (art. 26)
- doszczegółowieniu przepisów określających okresy przechowywania aktów
- wprowadzeniu obowiązku usuwania danych z systemów, wspomagających prowadzenie papierowej rejestracji stanu cywilnego, prowadzonych przed 2015 r. przez urzędy stanu cywilnego po przeniesieniu papierowego aktu stanu cywilnego do rejestru stanu cywilnego.

98. Ustawa z dnia 20 lutego 2015 r. o odnawialnych źródłach energii

Proponowana zmiana polegająca na dodaniu w art. 15 ust. 1a wynika z konieczności doprecyzowania skutku wykreślenia danych z rejestru poprzez wyraźne określenie, że wykreślenie z danego rejestru jest równoznaczne z fizycznym usunięciem z tego rejestru danych wykreślanego podmiotu. Pozwoli to uniknąć wątpliwości pojawiających się w związku z obecnym brzmieniem ww. przepisu czy dane podmiotu wykreślonego są nadal widoczne, ale np. z adnotacją „wykreślony” lub odpowiadającym jej oznaczeniem graficznym. Należy jednocześnie wskazać, że wszystkie wykreślane dane nadal znajdują się w złożonych do organu rejestrowego (Prezes Urzędu Regulacji Energetyki) wnioskach o wpis do rejestru, które

stanowią akta sprawy i jako takie są archiwizowane. W związku z tym zrezygnowano z określania w ustawie, przez jaki okres wnioski mają być przechowywane.

W związku z nałożonym przez rozporządzenie 2016/679 obowiązkiem wyraźnego określenia administratora danych osobowych proponuję wskazać, że wszystkie podmioty biorące udział w przetwarzaniu danych związanym z przekazywaniem wymienionych w przepisie informacji i sprawozdań są ich administratorami. Pozwoli to, przede wszystkim, uniknąć wątpliwości co do tego, który podmiot jest administratorem, a który podmiotem przetwarzającym. Wybierając takie rozwiązanie proponuję jednocześnie zrezygnować z zastępowania używanego w przepisach słowa „przekazuje" słowem „udostępnia". Wynika to z faktu, iż słowo „przekazuje" odnosi się do przekazania organowi (Prezesowi URE) kompleksowego dokumentu (określonego jako informacja lub sprawozdanie), w którym główną treść stanowią dane inne niż osobowe (zmiana w art. 22 ust. 3).

W związku z konstrukcją procedury wydawania świadectw pochodzenia oraz świadectw pochodzenia biogazu rolniczego, która może budzić wątpliwości, co do roli i obowiązków podmiotów w zakresie przetwarzania danych osobowych (wnioski są składane do Prezesa URE za pośrednictwem operatorów systemów) proponuję wyraźnie określić, że zarówno Prezes URE, jak i operatorzy są administratorami danych osobowych. Propozycja ta jest uzasadniona również tym, że operatorzy nie tylko przekazują wnioski, ale dokonują również ich częściowej weryfikacji, ich rola przy przetwarzaniu danych osobowych nie może zatem zostać pominięta (zmiana w art. 51 ust. 3).

99. Ustawa z dnia 25 czerwca 2015 r. o leczeniu niepłodności

Projektowana zamiana dotyczy przepisów odnośnie zasad przetwarzania danych w Rejestrze Dawców Komórek Rozrodczych i Zarodków oraz ogólnych zasad przetwarzania danych związanych z wykonywaniem zadań ośrodka medycznie wspomaganej prokreacji i banku komórek rozrodczych i zarodków. Wynika z konieczności dostosowania przepisów ustawy z dnia 25 czerwca 2015 r. o leczeniu niepłodności (Dz. U. poz. 1087 z późn. zm.) do skutków wejścia w życie przepisów rozporządzenia 2016/679.

Obowiązujące przepisy w zakresie ochrony danych osobowych, w tym ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) zostaną zastąpione. Odwołania zawarte w ustawie z dnia 25 czerwca 2015 r. o leczeniu niepłodności do przepisów

ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz aktów wykonawczych musiały więc zostać dostosowane do nowej sytuacji prawnej.

100. Ustawa z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

101. Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej

Zmiana w art. art. 35 ust. 2 pkt 10:
Zmiana ma charakter dostosowawczy i związana jest ze zmianą organu właściwego w sprawach ochrony danych osobowych. Zmiana polega na zastąpieniu odwołania do Generalnego Inspektora Danych Osobowych odwołaniem do Prezesa Urzędu Ochrony Danych Osobowych.

Zmiana art. 35 ust. 7:
Propozycja uzupełnienia art. 35 ust. 7 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (dalej: „u.d.u.r.”) poprzez wskazanie Ubezpieczeniowego Funduszu Gwarancyjnego (obok Polskiej Izby Ubezpieczeń) jako podmiotu zobowiązanego do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia. Propozycja ma na celu potwierdzenie objęcia obowiązkiem zachowania tajemnicy ubezpieczeniowej również Ubezpieczeniowego Funduszu Gwarancyjnego, co jest związane m.in. z prowadzeniem przez UFG informatycznych baz danych, które obejmują informacje o wypłaconych odszkodowaniach i świadczeniach z umów ubezpieczenia. Należy wskazać, iż UFG przejęło część uprawnień do prowadzenia baz danych od Polskiej Izby Ubezpieczeń (art. 102a ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych). Przetwarzanie przez UFG danych sensytywnych wymaga w świetle rozporządzenia 2016/679 (art. 9 i 10) dodatkowych gwarancji praw i wolności. Objęcie UFG expressis verbis tajemnicą ubezpieczeniową będzie mogło być uznane za taką gwarancję.

Zmiana art. 38 ust. 6 i 8:

Propozycja zmiany brzmienia art. 38 ust. 6 i 8 u.d.u.r. dotyczy modyfikacji w zakresie sposobu udzielenia zgody przez osobę, której dane dotyczą. Wyrażenie wyraźnej zgody na przetwarzanie danych osobowych (w sytuacjach o których mowa w przedstawionym przepisach) przez osobę ubezpieczoną, osobę na której rachunek ma być zawarta umowa ubezpieczenia lub przedstawiciela ustawowego każdej z tych osób, wynika z art. 9 ust. 2 lit. a rozporządzenia 2016/679, który explicite wskazuje na konieczność pozyskania wyraźnej zgody.

Zaproponowana zmiana zapewni zgodność regulacji krajowych z regulacjami unijnymi. Ponadto, w określonych sytuacjach fakt udzielenia wyraźnej zgody może mieć bardziej praktyczne zastosowanie, niż fakt udzielenia pisemnej zgody, która w określonych sytuacjach losowych może być pozbawiona elementu wyraźnej świadomości osoby, która tej zgody udziela. Taki sposób rozumienia wymogu udzielenia wyraźnej zgody przewiduje również uzasadnienie wynikające z motywy 111 preambuły rozporządzenia 2016/679.

Ponadto, warunkiem wyrażenia zgody, zapewniającym jej wyraźny charakter są obowiązki nałożone na administratora dotyczące sposobu sformułowania klauzuli wyrażenia zgody. Dotyczą one jej przejrzystości i precyzyjnego sformułowania, co jest dodatkowym elementem, uzasadniającym wystarczający charakter wyraźnego udzielenia zgody, przez osobę, której dane dotyczą.

Zmiana art. 39 ust. 1:

Zmiana rekomendowana w odniesieniu do dyspozycji art. 39 u.d.u.r. dotyczy sposobu wyrażenia zgody przez podmiot danych na udostępnienie danych osobowych innym zakładom ubezpieczeń. Uzasadnione jest usunięcie wymogu formy pisemnej (pisemnego żądania) w odniesieniu do wyrażania zgody na udostępnienia danych osobowych.

Postulat ten wydaje się być zasadny nie tylko na gruncie omówionego, w odniesieniu do propozycji zmiany art. 38 u.d.u.r., wymogu uzyskania zgody a nie pisemnej zgody osoby, której dane dotyczą, ale również na gruncie art. 43 u.d.u.r., który przewiduje możliwość tworzenia dokumentów – ale w konsekwencji nakładający obowiązki na zakład ubezpieczeń należytego ich utrwalenia i zabezpieczenia – dotyczących zawierania i wykonywania umów ubezpieczenia w postaci elektronicznej. Należy bowiem podkreślić, że wprowadzenie postaci elektronicznej jest odzwierciedleniem postulatów wysuwanych przez środowisko ubezpieczeniowe, związanych z koniecznością dostosowania regulacji prawnych do postępującego procesu

cyfryzacji. Zmiana jest również zgodna z art. 6 ust. 1 lit. a w zw. z art. 7 rozporządzenia 2016/679, który nie odwołuje się do wymogu pisemności zgody osoby, której dane dotyczą.

Zmiana art. 41 ust. 1, 1a, 1b, 2:

Modyfikacja zaproponowana do brzmienia art. 41 ust. 1 u.d.u.r. odnosi się do usunięcia przepisów odnoszących się jedynie do możliwości zbierania danych osobowych, a zastąpienie go obowiązkiem zbierania danych w celu wypełnienia obowiązku prawnego ciążącego na administratorze.

Zmiana wynika z regulacji zawartej w art. 6 ust. 1 lit. c rozporządzenia 2016/679, stanowiącej że administrator jest zobowiązany do przetwarzania danych w celu wypełnienia ciążącego na nim obowiązku prawnego. Należy podkreślić, że przetwarzanie danych osobowych osób korzystających z usług ubezpieczeniowych oferowanych przez administratora nie jest uznawane za przysługujące mu prawo, ale za obowiązek związany z zapewnieniem kompleksowej i profesjonalnej jakości świadczonych usług.

Propozycja dodania do art. 41 ust. 1a u.d.u.r. jest uzasadniona ze względu na konieczność doprecyzowania regulacji ustawowej w odniesieniu do prawnie dopuszczalnego zakresu przetwarzanych danych, w tym szczególnych kategorii danych osobowych (danych dotyczących zdrowia) w celu oceny ryzyka ubezpieczeniowego lub wykonania umowy ubezpieczenia.

Brzmienie art. 41 ust. 1b u.d.u.r. stanowi uzupełnienie treści z art. 41 ust. 1 i 2 związanej z przetwarzaniem danych osobowych w toku zawierania i realizacji umów ubezpieczeniowych, w kontekście możliwości przyznania zakładom ubezpieczeń zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania osób, których dane dotyczą. Regulacja zaproponowana na gruncie art. 41 ust. 3 u.d.u.r. przyznaje zakładom ubezpieczeń możliwość zautomatyzowanego podejmowania decyzji, w tym profilowania, która wprost wynika z uprawnienia z art. 22 ust. 2 lit. b rozporządzenia 2016/679. Art. 22 ust. 2 lit. b rozporządzenia RODO umożliwia dostosowanie regulacji krajowych, które zezwolą administratorom na przetwarzanie danych osobowych w sposób umożliwiający zautomatyzowane podejmowanie decyzji, w tym profilowanie, pod warunkiem wdrożenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Mając to na uwadze należy szczególnie podkreślić fakt, że brzmienie art. 41 ust. 1b u.d.u.r. jest tylko możliwością przyznaną zakładom ubezpieczeń do dokonywania zautomatyzowanego podejmowania decyzji, w tym profilowania jedynie w celu oceny ryzyka ubezpieczeniowego, uzasadnionej ponadto specyfiką prowadzonej regulowanej działalności. Potencjalne wątpliwości co do ryzyka przetwarzania danych osobowych czy ich ewentualnego udostępnienia zostaje zminimalizowane, ze względu na fakt, że zakład ubezpieczeń, który może dokonywać profilowania i podejmowania zautomatyzowanych decyzji, jest związany tajemnicą ubezpieczeniową, a jego działalność jest nadzorowana przez Komisję Nadzoru Finansowego.

Zmiana ust. 2 jest związana z koniecznością uregulowania przesłanek wyłączenia – tak jak w obecnej regulacji – obowiązku informacyjnego. Pozyskiwanie i przetwarzanie danych osobowych osób, objętych umową ubezpieczenia jest bezpośrednio związane z regulacją zawartą w art. 14 ust. 5 lit. c rozporządzenia RODO, który dopuszcza przetwarzanie danych osobowych z pominięciem obowiązku informacyjnego, m. in. w przypadku gdy pozyskiwanie lub ujawnianie tych danych jest wyraźnie uregulowane prawem państwa członkowskiego. Uwzględniając powyższe należy wskazać, że propozycja zmiany art. 41 ust. 2 u.d.u.r., który wyraźnie wskazuje na okoliczność przetwarzania danych osobowych w związku z zawieraniem i wykonywaniem umów ubezpieczenia, bezpośrednio koresponduje z regulacją z art. 14 ust. 5 lit. c rozporządzenia 2016/679.

Tym samym administrator danych przetwarzając dane osobowe związane z zawieraniem i wykonywaniem umów ubezpieczenia, w zakresie i na zasadach przewidzianych w art. 41 ust. 1 i 1a u.d.u.r. jest zwolniony z konieczności realizacji obowiązku informacyjnego w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, z uwagi na podstawę prawną wynikającą z tej regulacji ustawowej. Należy również wskazać, że zakład ubezpieczeń pełniący funkcję administratora danych jest zobowiązany do podjęcia środków zapewniających odpowiedni poziom bezpieczeństwa przetwarzanych danych objętych zakresem tajemnicy ubezpieczeniowej.

102. Ustawa z dnia 25 września 2015 r. o zawodzie fizjoterapeuty

W art. 12 ust. 9 ustawy z dnia 25 września 2015 r. o zawodzie fizjoterapeuty (Dz. U. poz. 1994), znajduje się odwołanie do obecnie obowiązującej „ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. W związku z wejściem w życie rozporządzenia 2016/679

oraz nowej ustawy o ochronie danych osobowych odwołanie do obecnie obowiązującej ustawy o ochronie danych osobowych stanie się nieaktualne, w związku z czym konieczne stało się uchylenie odesłania.

103. Ustawa z dnia 9 października 2015 r. o produktach biobójczych

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

104. Ustawa z dnia 28 stycznia 2016 r. – Prawo o prokuraturze

W związku z tym, że administratorem przetwarzanych danych osobowych jest Prokurator Generalny odpowiedniej korekty dokonano w art. 13 § 5. Ponieważ rozporządzenie nie przewiduje konieczności zgłaszania rejestru danych należało uchylić § 2 w art. 191, który przewidywał wyłączenie konieczności jego rejestracji.

Z uwagi na to, że zawarte w art. 2 ust. 2 lit. d rozporządzenia 2016/679 wyłączenie jego stosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, które uregulowano Dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, nie obejmuje swym zakresem części zadań i czynności wykonywanych przez kuratorów sądowych, konieczna jest zmiana ustawy z dnia 27 lipca 2001 r. o kuratorach sądowych (Dz. U. z 2014 r. poz. 795).

Kuratorska służba sądowa funkcjonalnie i organizacyjnie usytuowana jest w sądach. Zgodnie z treścią przepisu art. 147 § 2 in principio ustawy – Prawo o ustroju sądów powszechnych kuratorzy sądowi działają w sądach (kuratorzy rodzinni i kuratorzy dla dorosłych), stanowiąc służbę kuratorską. Zakres czynności został zaś wskazany in fine cyt. przepisu określając, że kuratorzy sądowi wykonują czynności o charakterze wychowawczo-resocjalizacyjnym i profilaktycznym oraz inne czynności określone w przepisach szczególnych. Jak wynika z treści tego przepisu, ma on charakter ogólny, stanowi jedynie

częściowe powtórzenie art. 1 ust. 1 ustawy o kuratorach sądowych, odsyłając jednocześnie do przepisów szczególnych.

Ażeby w pełni odkodować zakres czynności wykonywanych przez kuratorów sądowych (zawodowych i społecznych), należy posiłkować się zarówno ustawą o kuratorach sądowych, jak i wskazaniem pełnego zakresu czynności, w szczególności tych, które nie mieszczą się w zakresie wyłączenia opisanego w art. 2 ust. 2 lit. d cyt. rozporządzenia.

Należy podkreślić, że kuratorzy sądowi pełnią swoje czynności zawodowo (kuratorzy zawodowi) albo społecznie (kuratorzy społeczni), a zasady organizacji służby i wykonywania obowiązków przez kuratorów sądowych oraz status kuratorów sądowych określa odrębna ustawa (154 §1 i 2 ustawy – Prawo o ustroju sądów powszechnych). Zgodnie z treścią ustawy o kuratorach sadowych, kuratorzy sądowi realizują określone przez prawo zadania o charakterze wychowawczo – resocjalizacyjnym, diagnostycznym, profilaktycznym i kontrolnym, związane z wykonywaniem orzeczeń sądu (art. 1 tej ustawy). Prima facie zdawać się może, że wszystkie opisane zadania, mieszczą się w zakresie wyłączenia, o którym mowa, tj. przetwarzania danych osobowych przez właściwe organy, tj. zapobiegania przestępczości, prowadzenia postępowań przygotowawczych lub wykonywania kar, jednakże zakres szczególnych czynności wzbudza uzasadnione wątpliwości, które stały się przedmiotem rozważań Trybunału Konstytucyjnego w sprawie U 2/14, w której badał zgodność z Konstytucją RP niektórych przepisów Rozporządzenia Ministra Sprawiedliwości z dnia 26 lutego 2013 r. w sprawie sposobu wykonywania obowiązków i uprawnień przez kuratorów sądowych w sprawach karnych wykonawczych (Dz. U. z 2013, poz. 335).

W wyroku z dnia 16 grudnia 2014 r. Trybunał Konstytucyjny orzekł między innymi o niezgodności § 5 ust. 5 oraz § 25 ust. 5 tego rozporządzenia z art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz z art. 92 ust. 1 zdanie pierwsze Konstytucji RP. Co istotne, Trybunał Konstytucyjny zajął się ta kwestią wpadkowo, będąc związanym granicami wniosku i skoncentrował się na uprawnieniach kuratorów do przetwarzania danych osobowych tylko w zakresie, w jakim byli oni zobowiązani do przekazywania funkcjonariuszom policji informacji o powierzeniu lub zakończeniu dozoru nad skazanym za przestępstwa polegającego na użyciu przemocy lub groźby bezprawnej. W uzasadnieniu wyroku TK wskazał m.in., że:„Nie ma zatem przepisów ustawowych, które zezwalałyby kuratorowi na przetwarzanie danych dotyczących skazania za przestępstwo popełnione z użyciem przemocy lub groźby bezprawnej w postaci przekazywania

tych danych komendantowi powiatowemu Policji. Podstawą do tego nie są w szczególności ogólne przepisy określające prawa i obowiązki kuratorów, przywołane przez Ministra Sprawiedliwości w piśmie z 13 maja 2014 r., zawarte m.in. w art. 9 pkt 4 i 5 ustawy o kuratorach sądowych (na podstawie których kurator ma dostęp do dokumentacji dotyczącej podopiecznych oraz ma prawo żądać od Policji pomocy w wykonywaniu czynności służbowych). Nieuprawnione jest także twierdzenie Ministra Sprawiedliwości, że ustawową podstawą do przetwarzania przez kuratora danych, o których mowa w § 5 ust. 5 i § 25 ust. 5 rozporządzenia z 26 lutego 2013 r., są przepisy ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, ze zm.), przewidujące uprawienie Policji do gromadzenia i przetwarzania danych osobowych w celu realizacji ustawowych zadań. Owszem, są to regulacje spełniające kryterium przyjęte w art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, lecz ich adresatem nie są kuratorzy, lecz Policja. Są one zatem ustawowym zezwoleniem na przetwarzanie danych wrażliwych przez Policję w celu realizacji jej ustawowych zadań, przede wszystkim zapobiegania i wykrywania przestępstw oraz identyfikacji osób.”

Wprawdzie wskazane rozporządzenie uchylono, a w jego miejsce przyjęto rozporządzenie Ministra Sprawiedliwości z dnia 13 czerwca 2016 r. w sprawie sposobu i trybu wykonywania czynności przez kuratorów sądowych w sprawach karnych wykonawczych (Dz. U. z 2016 r. poz. 969 – dalej: rozporządzenie), to jednak przepisy w tej mierze zostały recypowane z rozporządzenia z 26 lutego 2013 r., zatem rozważania Trybunału Konstytucyjnego, z racji braku zmian ustawowych należy uznać za aktualne.

Biorąc pod uwagę kierunek orzecznictwa Trybunału Konstytucyjnego, należy przyjąć, że szereg innych przepisów z dnia 13 czerwca 2016 r., może w przyszłości budzić uzasadnione wątpliwości, co do zgodności z ustawą o ochronie danych osobowych oraz rozporządzenia RODO, m.in. w zakresie:

1) przesyłania jednostce Policji właściwej dla miejsca stałego pobytu skazanego informacji o oddaniu pod dozór skazanego za przestępstwo z użyciem przemocy lub groźby bezprawnej (§ 4 ust. 1 pkt 1 rozp.),

2) uzyskiwania numeru telefonu lub adres poczty elektronicznej skazanego, umożliwiające mu kontaktowanie się ze skazanym podczas dozoru; jeżeli skazany wyraził na

to zgodę, wezwań, zawiadomień lub przekazywania informacji kurator sądowy może dokonywać także telefonicznie lub za pośrednictwem poczty elektronicznej (§ 5 ust. 3 rozp.),

3) zasięgania informacji o skazanym w placówkach oświatowych i oświatowo-wychowawczych,

4) zaznajamiania się z wynikami leczenia, rehabilitacji lub terapii skazanego, a także utrzymywania kontaktu z osobami prowadzącymi leczenie, rehabilitację, terapię lub inne formy specjalistycznego oddziaływania oraz zapoznawania się z ewentualnymi wskazówkami tych osób dotyczącymi przebiegu dozoru a następnie konsultowania sposobu sprawowania dozoru z osobami, o których mowa; podejmowania działań mających na celu przestrzeganie przez skazanego zaleceń lekarskich bądź zaleceń innych specjalistów z zakresu rehabilitacji lub terapii, sprawując dozór wobec sprawcy przestępstwa popełnionego w stanie ograniczonej poczytalności lub w związku z uzależnieniem od alkoholu, środka odurzającego lub innego podobnie działającego środka (§ 15 ust. 1-4 rozp.);

5) nawiązania współpracy […] z organizacjami pozarządowymi funkcjonującymi na terenie miejsca zamieszkania osób pokrzywdzonych w celu uzyskania w niezbędnym zakresie informacji o rodzinie dotkniętej przemocą (§ 16 ust. 1 pkt 2 rozp.), sprawując dozór wobec sprawcy przemocy w rodzinie;

6) w zakresie wymiany informacji w czasie uczestniczenia w posiedzeniach zespołu interdyscyplinarnego i grupy roboczej, o których mowa w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie (Dz. U. z 2015 r. poz. 1390) (§ 16 ust. 1 pkt 5 rozp.), sprawując dozór wobec sprawcy przemocy w rodzinie.

Bezpośrednią przyczyną powstałych wątpliwości wydają się być kolejne zmiany w treści ustawy o ochronie danych osobowych. Pierwotne brzmienie przepisu art. 27 ust. 2 pkt 4 tejże ustawy pozwalało na pozyskiwanie, gromadzenie i przetwarzanie danych osobowych o ile „dane osobowe są niezbędne do wykonywania określonych prawem zadań, realizowanych dla dobra publicznego”, które w związku z treścią art. 9 pkt 5 ustawy o kuratorach sądowych gwarantował kuratorom zawodowym możliwość „żądania od Policji oraz innych organów lub instytucji państwowych, organów samorządu terytorialnego, stowarzyszeń i organizacji społecznych w zakresie ich działania, a także od osób fizycznych pomocy w wykonywaniu czynności służbowych”.

Obecnie obowiązujący art. 27 ust. 2 ustawy o ochronie danych osobowych. wyklucza gromadzenie i przetwarzanie danych przez kuratorów sądowych wykonujących zarówno orzeczenia w sprawach karnych, m.in. w opisanym zakresie, a także kuratorów wykonujących orzeczenia w sprawach rodzinnych i nieletnich. Zaś zgodnie z art. 27 ust. 2 pkt 2 tej ustawy przetwarzanie danych wrażliwych jest dopuszczalne o ile „przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

Mając na uwadze powyższe, w ustawie o kuratorach sądowych proponuje się dodanie art. 9a, art. 35a i art. 35b, a także określenie na nowo treści przepisu art. 87 ust. 3.

Wskazana interwencja legislacyjna wydaje się konieczna także na gruncie art. 5 ust. 1 lit. b rozporządzenia 2016/679 zd. pierwsze, zgodnie z treścią którego dane osobowe muszą być zbieranie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Z tych samych powodów należy wskazać, iż wprowadzenie proponowanych przepisów znajduje uzasadnienie w związku z treścią art. 6 ust. 3 lit. b w zw. z art. 6 ust. 1 lit. c i e rozporządzenia 2016/679, w którym określono, że podstawa przetwarzania, która jest niezbędna do wypełniania obowiązku prawnego ciążącego na administratorze oraz niezbędna do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, musi być określona w prawie państwa członkowskiego, któremu podlega administrator.

105. Ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowaniu dzieci

Zmiana o charakterze czysto technicznym polegająca na usunięciu odesłania w art. 14 ust. 3 do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

106. Ustawa z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych

Zmiana o charakterze porządkowym, usunięto w przepisie odesłanie do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ ustawa ta zostanie uchylona.

107. Ustawa z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań z zakresu informatyzacji działalności organów Krajowej Administracji Skarbowej

Propozycja przewidziana w zmienianym art. 17 ust. 1 dopuszcza, w sytuacji przetwarzania danych przez spółkę celową, możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i art. 34 RODO. Ograniczenie praw podmiotów danych jest możliwe na podstawie art. 23 ust. 1 lit. d i e RODO, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym 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 oraz 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. W przypadku art. 17 ust. 1 ograniczenie to zostało zastosowane w zakresie niezbędnym do realizowania zadań spółki celowej utworzonej w celu realizacji niektórych projektów informatycznych o publicznym zastosowaniu z zakresu spraw należących do działu administracji rządowej finanse publiczne ustawowych przez organy podatkowe. Celem projektów realizowanych przez spółkę celową jest zapewnienie organom Krajowej Administracji Skarbowej systemów teleinformatycznych wspierających wykrywanie naruszenia przepisów prawa podatkowego, w oparciu o dane uzyskiwane z systemów teleinformatycznych ministra właściwego do spraw finansów publicznych oraz organów Krajowej Administracji Skarbowej. W związku z tym uznać należy, że spełniona jest przesłanka ważnego celu leżącego w ogólnym interesie publicznym uzasadniająca wprowadzenie wymienionych ograniczeń.

Przepis zawiera ponadto o 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.

Zmiana w art. 18 ust. 1, 2 i 6 ma charakter dostosowujący i polega na zastąpieniu odwołania ogólnie do przepisów o ochronie danych osobowych zamiast obecnie obowiązujących przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

108. Ustawa z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym

W ustawie tej zaproponowano następujące zmiany:

1) w związku z tym, że administratorem danych osobowych przetwarzanych w Rejestrze Sprawców na Tle Seksualnym jest Minister Sprawiedliwości – odpowiedniej korekty wymaga art. 5 ust. 2;

2) ze względu na to, że zgromadzone w Rejestrze dane będą przetwarzane, obok celu pierwotnego, także dla potrzeb badań naukowych lub statystycznych, dodając art. 17 ust. 3a proponuje się wyłączyć stosowanie co do danych przetwarzanych dla tych celów:

– art. 15 rozporządzenia 2016/679 zapewniającego osobie, której dane dotyczą, prawo dostępu do informacji od administratora danych, czy przetwarzane są jej dane osobowe,

– art. 16 rozporządzenia 2016/679 przyznającego osobie, której dane dotyczą, prawo do sprostowania danych,

– art. 18 rozporządzenia 2016/679 przyznającego osobie, której dane dotyczą, prawo żądania od administratora ograniczenia przetwarzania jej danych osobowych w określonych przypadkach,

– art. 21 rozporządzenia 2016/679 przyznającego osobie, której dane dotyczą, prawo wniesienia sprzeciwu, z przyczyn związanych z jej szczególną sytuacją, wobec przetwarzania dotyczących jej danych osobowych.

Podstawę wyłączeń stanowi art. 89 ust. 2 rozporządzenia 2016/679. Ich wprowadzenie podyktowane jest koniecznością zapewnienia niezakłóconej realizacji przetwarzania danych zgromadzonych w Rejestrze do celów badań naukowych lub statystycznych, które to badania, z uwagi na rodzaj przetwarzanych danych, mogą mieć niebagatelne znaczenie także dla realizacji głównego celu Rejestru, tj. zapobieżenia zagrożeniom przestępczością na tle seksualnym.

Z drugiej strony wskazać należy, że rozwiązania przewidziane w ustawie zapewniają prawa i wolności osoby, której dane dotyczą, zgodnie z rozporządzeniem (art. 89 ust. 1 rozporządzenia 2016/679). Mianowicie ustawa przewiduje w art. 19 szczegółową procedurę korygowania danych nieprawidłowych lub błędnie wprowadzonych. Ustawa gwarantuje nadto każdej osobie prawo do uzyskania informacji z Rejestru, czy jej dane zostały zgromadzone w Rejestrze (art. 12 pkt 8 ustawy).

109. Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej

Zgodnie z art. 35 ustawy o Krajowej Administracji Skarbowej Centralny Rejestr Danych Podatkowych (CRDP) służy do przetwarzania danych wynikających, w szczególności z: deklaracji podatkowych, decyzji, postanowień, tytułów wykonawczych oraz danych zgromadzonych w Centralnym Rejestrze Podmiotów – Krajowej Ewidencji Podatników.

Przepis art. 23 rozporządzenia 2016/679 dopuszcza możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i art. 34, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym m.in. 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.

Biorąc pod uwagę powyższą przesłankę w związku z ważnym interesem gospodarczym RP związanym z kwestiami budżetowym i podatkowym konieczne stało się dodanie regulacji, zgodnie z którą do przetwarzania danych osobowych w CRDP nie stosuje się art. 12-22 i art. 34 rozporządzenia 2016/679.

Zmiana zaproponowana w art. 45 ust. 1 ustawy o Krajowej Administracji Skarbowej polega na wpisaniu jako podstawy przetwarzania danych osobowych zbieranych i wykorzystywanych przez organy KAS w celu realizacji ustawowych zadań, o których mowa w art. 2 ust. 1 pkt 1 (realizacja dochodów z podatków, opłat oraz niepodatkowych należności budżetowych, jak również innych należności, na podstawie odrębnych przepisów, z wyjątkiem podatków i należności budżetowych, w zakresie których właściwe są inne organy), pkt 2 (realizacja dochodów z należności celnych oraz innych opłat związanych z przywozem i wywozem towarów), pkt 6 (wykonywanie egzekucji administracyjnej należności pieniężnych oraz wykonywanie zabezpieczenia należności pieniężnych) i pkt 8

(wykonywanie audytu, czynności audytowych i urzędowego sprawdzenia), w miejsce ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. z 2016 r. poz. 922) przepisów rozporządzenia 2016/679.

Z kolei propozycja dodania w art. 45 ust. 1a dopuszcza, w sytuacji opisanej w ust. 1, możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i art. 34 rozporządzenia 2016/679. Ograniczenie praw podmiotów danych jest możliwe na podstawie art. 23 ust. 1 lit. e rozporządzenia 2016/679, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym 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. W przypadku art. 45 ust. 1a ograniczenie to zostało zastosowane z uwagi na interes finansowy Unii oraz budżetu państwa w tym kwestie budżetowe i podatkowe.

Zmiana zaproponowana w art. 47 ust. 1 polega, podobnie jak zmiana dokonana w art. 45 ust. 1, na wpisaniu w miejsce przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jako podstawy przetwarzania danych osobowych, przepisów rozporządzenia 2016/679.

Natomiast ust. 2 w miejsce przywołanych przepisów art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wprowadza się odpowiadające mu przepisy art. 9 ust. 1 i art. 10 rozporządzenia 2016/679 (przetwarzanie szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa).

Propozycja dodania ust. 1a w art. 127 dopuszcza, w sytuacji opisanej w ust. 1, możliwość ograniczenia praw podmiotów danych wskazanych w art. 12-22 i art. 34 rozporządzenia 2016/679. Ograniczenie praw podmiotów danych jest możliwe na podstawie art. 23 ust. 1 lit. d i e rozporządzenia 2016/679, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym 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 oraz 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. W przypadku art. 127 ust. 1a ograniczenie to zostało zastosowane w zakresie niezbędnym do realizacji zadań KAS, o których mowa w art. 113 ust. 1 ustawy o Krajowej Administracji Skarbowej.

Przepisy art. 35, art. 47a i art. 127 zawierają też, 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.

110. Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe

W proponowanych zmianach ustawy zgodnie z propozycją ministra właściwego do spraw kultury i dziedzictwa narodowego, uwzględniono brzmienie art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), który wymaga, aby przepis prawa krajowego określał obowiązek, którego realizacja wiązałaby się z koniecznością przetwarzania danych osobowych oraz rodzaj danych osobowych przetwarzanych w ramach poszczególnych zadań.

Z tego względu proponuje się wprowadzenie do ustawy przepisów określających obowiązki przetwarzania danych w związku z wykonywaniem określonych w tych ustawach zadań.

Na podstawie art. 23 rozporządzenia 2016/679 proponuje się ograniczenie praw podmiotu danych, o których mowa w art. 12 i 15 rozporządzenia 2016/679, w ten sposób, że korespondencja oraz dostęp do danych byłyby realizowane bezpłatnie raz na 6 miesięcy. Częstsza realizacja wiązałaby się z koniecznością wniesienia opłaty równej kosztom sporządzenia odpowiedzi lub kopii danych. Propozycja jest uzasadniona interesem finansowym państwa: minister właściwy do spraw kultury i ochrony dziedzictwa narodowego w zakresie, w jakim sprawuje nadzór nad szkolnictwem artystycznym, inne jednostki nadzoru nad tym

szkolnictwem, szkoły i placówki artystyczne jako podmioty publiczne narażone byłyby na poniesienie znacznych kosztów w przypadku realizacji praw przewidzianych w powyższych przepisach bez ograniczeń. Z tego samego powodu proponuje się ograniczenie obowiązku zawiadamiania podmiotu danych o naruszeniu ochrony, na podstawie art. 34 rozporządzenia 2016/679, zobowiązując zarazem administratora danych do umieszczenia na swojej stronie internetowej lub w Biuletynie Informacji Publicznej komunikatu o zaistniałym naruszeniu nie później niż 72 godziny od stwierdzenia naruszenia. Wprowadzenie ograniczeń praw określonych w art. 13 i 14 (prawo do informacji) oraz obowiązku, o którym mowa w art. 5 ust. 2 rozporządzenia 2016/679 (dokumentowanie przestrzegania przepisów o ochronie danych) jest konieczne nie tylko z uwagi na nadmierny koszt ale również inne niewspółmierne nakłady.

Należy podkreślić, że administrator byłby zobowiązany do publicznego poinformowania o wprowadzonych ww. ograniczeniach i włączeniach na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

111. Ustawa z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami

Zmiana ma charakter dostosowujący i polega na zastąpieniu odwołania do odpowiednich przepisów rozporządzenia 2016/679 w miejsce obecnie obowiązujących przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

W rozdziale 3 zawarto przepisy dostosowujące oraz przejściowe.

Proponuję się, aby w celu zapewnienia ciągłości wykonywania funkcji gwarantującej przestrzeganie przepisów o ochronie danych osobowych w danym podmiocie, osoby wykonujące w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji wykonywały funkcję inspektora ochrony danych osobowych do dnia 1 września 2018 r. W tym czasie administrator danych osobowych lub podmiot przetwarzający powinien zawiadomić Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu inspektora ochrony danych osobowych zgodnie z procedurą wskazaną w art. 5 ustawy o ochronie danych osobowych albo w tym terminie obowiązany jest przekazać Prezesowi Urzędu Ochrony Danych Osobowych informację, że dotychczasowy administrator bezpieczeństwa informacji nie pełni u niego funkcji inspektora ochrony danych osobowych. Jednocześnie jeżeli w tym czasie, czyli do dnia 1 września 2018 r., administrator bezpieczeństwa informacji nie zgłosi danych kontaktowych dotychczasowego administratora bezpieczeństwa informacji do Prezesa Urzędu Ochrony

Danych Osobowych, to ten administrator przestaje pełnić funkcję inspektora ochrony danych. Warto również zauważyć, że w okresie przejściowym czyli do dnia 1 września 2018 r. administrator danych osobowych może w każdym czasie zawiadomić Prezesa Urzędu Ochrony Danych Osobowych, że administrator bezpieczeństwa informacji nie pełni u niego funkcji inspektora ochrony danych.

Zastosowanie konstrukcji zgodnie z którą dotychczasowy administrator bezpieczeństwa informacji pełni automatycznie rolę inspektora ochrony danych osobowych tylko przez pewien dość krótki, określony czas podyktowane zostało przede wszystkim tym by zapewnić ciągłość wykonywania funkcji, która ma gwarantować przestrzeganie danych osobowych ale także tym, że zgodnie z rozporządzeniem 2016/679 na inspektorów ochrony danych osobowych nałożone zostaną znacznie większe wymania niż te które obecnie obowiązani są spełniać administratorzy bezpieczeństwa informacji. Rozporządzenie 2016/679 wprowadza wymóg kwalifikacji zawodowych inspektora ochrony danych osobowych, na które składają się: wiedza fachowa oraz umiejętności potrzebne do wykonywania zadań inspektora ochrony danych osobowych, określonych w rozporządzeniu 2016/679. W obecnym stanie prawnym administrator bezpieczeństwa informacji musi jedynie posiadać wiedzę w zakresie ochrony danych osobowych, która odnosi się do obecnych przepisów o ochronie danych osobowych. Również zakres jego zadań nie pokrywa się w pełni z zadaniami inspektora ochrony danych osobowych.

W świetle powyższego w ocenie projektodawcy istnieje konieczność zweryfikowania dotychczasowych administratorów bezpieczeństwa informacji pod kątem nowych wymagań kwalifikacyjnych.

W kolejnych przepisach wskazano, że Biuro Generalnego Inspektora Ochrony Danych Osobowych staje się Urzędem Ochrony Danych Osobowych. Przewidziano również, że wszyscy pracownicy zatrudnieni w Biurze Generalnego Inspektora Ochrony Danych Osobowych stają się pracownikami Urzędu Ochrony Danych Osobowych.

Wskazano również, że mienie skarbu państwa będące we władaniu Generalnego Inspektora staje się mieniem Prezesa Urzędu, również wszelkie należności i zobowiązania Generalnego Inspektora stają się należnościami i zobowiązaniami Prezesa Urzędu.

W art. 138 i 1139 ustawy wprowadzającej uregulowany został wpływ nowej ustawy na wszelkie postępowania wszczęte i niezakończone przed dniem wejścia w życie ustawy.

W art. 140 projektu uregulowano sytuację gdy Generalny Inspektor Ochrony Danych Osobowych, skorzystał ze swego uprawnienia przewidzianego w art. 19a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i skierował do danego podmiotu wystąpienie lub wniosek. Zgodnie z przepisem zaproponowanym w tym artykule, taki podmiot obowiązany jest udzielić odpowiedzi Prezesowi Urzędu w terminie 30 dni od dnia otrzymania wystąpienia lub wniosku.

Zgodnie z art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Generalny Inspektor obowiązany jest raz w roku złożyć Sejmowi sprawozdanie ze swojej działalności. W projektowanym przepisie przewidziano, że w przypadku gdy Generalny Inspektor do dnia wejścia w życie ustawy nie złoży sprawozdania, Prezes Urzędu obowiązany jest złożyć to sprawozdanie w terminie do dnia 31 lipca 2018 r.

Z uwagi na fakt, że zarówno rejestr zbiorów danych osobowych jak i rejestr administratorów bezpieczeństwa nie będą już prowadzone, ponieważ rozporządzenia 2016/679 nie przewiduje takiego obowiązku, w art. 143 i 144 projektu ustawy wskazano, że dane zgromadzone w tych rejestrach Prezes Urzędu przechowywał będzie przez okres 3 lat od dnia wejścia w życie ustawy.

Projekt ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych jest zgodny z prawem Unii Europejskiej.

Projekt ten nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt został umieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, oraz na stronie podmiotowej Biuletynu Informacji Publicznej Ministra Cyfryzacji.