ZASTĘPCA SZEFA
KANCELARII SEJMU
Adam Podgórski

Warszawa, dnia 11 kwietnia 2018 r.

GMS-WP-173-109/18

Przewodniczący
Konferencji Rektorów
Akademickich Szkół Polskich
Pan prof. dr hab. inż. Jan Szmidt

Szanowny Panie Przewodniczący

Z upoważnienia Marszałka Sejmu, uprzejmie przekazuję – w trybie art. 55 ust. 2 pkt 3 ustawy z dnia 27 lipca 2005 r. - Prawo o szkolnictwie wyższym (Dz.U.2017.2183 j.t. ze zm.) - rządowy projekt ustawy o ochronie danych osobowych, z prośbą o przedstawienie opinii.

Z poważaniem

PREZES RADY MINISTRÓW

Warszawa, dnia 5 kwietnia 2018 r.

RM-10-49-18

Pan Marek KUCHCIŃSKI
Marszałek Sejmu

Szanowny Panie Marszałku

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi

projekt ustawy o ochronie danych osobowych z projektami aktów wykonawczych.

Projekt ma na celu wykonanie prawa Unii Europejskiej.

W załączeniu przedstawiam także opinię dotyczącą zgodności proponowanych regulacji z prawem Unii Europejskiej.

Jednocześnie informuję, że do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Cyfryzacji.

Z poważaniem

M. Morawiecki

Warszawa, 4 kwietnia 2018 r.

[redacted]

Minister
Spraw Zagranicznych

DPUE.920.1409.2017/68/mp

dot.: RM-10-49-18 z 29.03.2018 r. (tekst ostateczny)

Pani
Jolanta Rusiniak
Sekretarz Rady Ministrów

Opinia
o zgodności z prawem Unii Europejskiej *projektu ustawy o ochronie danych osobowych*, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowna Pani Minister,

w związku z przedłożonym projektem ustawy pozwalam sobie wyrazić poniższą opinię.

1. Na podstawie art. 5 ust. 2 projektu ustawy wnioskodawca wprowadza ograniczenie stosowania art. 15 ust. 1 i 3 *rozporządzenia PE 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; RODO). Ograniczenie to polega na wprowadzeniu obowiązku wskazania przez osobę, której dane dotyczą, informacji pozwalających na wyszukanie jej danych osobowych w przypadku, gdy takie wyszukanie wymaga niewspółmiernie dużego wysiłku.

   Zwracam uwagę, że w związku z wątpliwościami co do zgodności z RODO, treść projektowanych art. 3-5 ustawy była konsultowana z Komisją Europejską, która negatywnie oceniła projektowany art. 5 ust. 2. Art. 15 RODO nie przewiduje możliwości ograniczenia praw z niego wynikających, jeżeli wykonanie obowiązku zapewnienia dostępu do danych wiąże się z niewspółmiernie dużym wysiłkiem. Ponadto wprowadzane ograniczenie nie spełnia wymagań wynikających z art. 23 RODO i w związku z tym nie może być uzasadnione na podstawie tego przepisu. W konsekwencji projektowany przepis należy uznać za niezgodny z art. 15 RODO.

   Uwzględniając powyższe proponuję usunąć art. 5 ust. 2 z projektu ustawy.

2. Do obecnego art. 6 wnioskodawca dodał pkt 2, zgodnie z którym przepisów ustawy oraz RODO nie stosuje się do działalności służb specjalnych w rozumieniu art. 11 *ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*.

   Należy zauważyć, że przepis ten ma na celu wprowadzenie podmiotowego wyłączenia od stosowania RODO dla pięciu służb specjalnych: ABW, AW, SKW, SWW i CBA, gdyż

wyłącza on stosowanie RODO odnośnie do całej działalności tych służb. Trzeba przy tym podkreślić, że wyłączenie to zostało wprowadzone nie tylko w zakresie działalności służb specjalnych nieobjętej prawem UE (bezpieczeństwo narodowe) ale również w zakresie ich działalności objętej prawem UE (np. zatrudnienie).

W ocenie MSZ projektowany przepis jest niezgodny z art. 2 ust. 1 RODO, który określa materialny zakres stosowania RODO w związku z art. 2 ust. 2 RODO wprowadzającym z kolei katalog dziedzin, do których RODO nie ma zastosowania.

Zgodnie bowiem z art. 2 ust. 1 RODO, rozporządzenie to ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Natomiast RODO nie ma zastosowania do przetwarzania danych osobowych wyłączenie w następujących przypadkach (art. 2 ust. 2 RODO):

a) w ramach działalności nieobjętej prawem UE;

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

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

d) 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.

Ponadto przypominam, że kwestia możliwości podmiotowego wyłączenia służb specjalnych od stosowania przepisów RODO została skonsultowana z Komisją Europejską. Komisja przedstawiła swoje stanowisko, zgodnie z którym tego typu wyłączenie jest niezgodne z RODO.

Uwzględniając powyższe proponuję usunąć art. 6 pkt 2 z projektu ustawy.

3. MSZ podtrzymuje uwagę zgłoszoną do obecnego art. 97 projektu ustawy (wcześniej art. 98).

Projektowany art. 97 przewiduje, że sąd krajowy w postępowaniu o naprawienie szkody będzie związany ustaleniami Prezesa UODO albo sądu administracyjnego co do stwierdzenia naruszenia przepisów o ochronie danych osobowych. Sąd krajowy zostanie zatem pozbawiony możliwości samodzielnego ustalenia stanu faktycznego i prawnego w danej sprawie.

Przepis ten jest zdaniem MSZ niezgodny z przepisami rozdziału VIII RODO pt. „Środki ochrony prawnej, odpowiedzialność i sankcje", ponieważ istotnie narusza skuteczność stosowania art. 79 (prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu) i 82 RODO (prawo do odszkodowania).

Po pierwsze należy zwrócić uwagę, że art. 79 ust. 1 RODO stanowi, że bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy RODO zostały naruszone w wyniku

przetwarzania jej danych osobowych z naruszeniem RODO. Tymczasem projektowany art. 97 poważnie ogranicza możliwość dochodzenia roszczeń przed sądem.

Po drugie art. 82 RODO przewiduje, że każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Należy w tym miejscu zauważyć, że odszkodowania można dochodzić wyłączenie przed sądem, a projektowany art. 97 ustawy może nawet całkowicie pozbawić możliwości dochodzenia odszkodowania w przypadku, gdy Prezes UODO stwierdzi brak naruszenia.

Uwzględniając powyższe proponuję usunąć art. 97 z projektu ustawy.

Projekt ustawy jest zgodny z prawem Unii Europejskiej z zastrzeżeniem uwag zawartych w niniejszej opinii.

Z poważaniem

z up. Ministra Spraw Zagranicznych
Piotr Wawrzyk
Podsekretarz Stanu

Do wiadomości:
Pan Marek Zagórski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Projekt ustawy o ochronie danych osobowych

Etap: RM

Projekt wykonuje 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; dalej: RODO)

Termin wdrożenia: 25 maja 2018 r.

Resort wnoszący: Ministerstwo Cyfryzacji

Minister odpowiedzialny za projekt ustawy: Sekretarz Stanu Marek Zagórski

Projekt ustawy	RODO
Art. 5 ust. 2 W przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 rozporządzenia nr 2016/679, wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, administrator wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Przepis art. 64 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio.	Artykuł 15 Prawo dostępu przysługujące osobie, której dane dotyczą 1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji: a) cele przetwarzania; b) kategorie odnośnych danych osobowych; c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu; e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania; f) informacje o prawie wniesienia skargi do organu nadzorczego; g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle; h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. 2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma

	prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem. 3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. 4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych. Artykuł 23 Ograniczenia 1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 - o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 - jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym: a) bezpieczeństwu narodowemu; b) obronie; c) bezpieczeństwu publicznemu; d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom; e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu; f) ochronie niezależności sądów i postępowania sądowego; g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu; h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) - e) oraz g);

	i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób; j) egzekucji roszczeń cywilnoprawnych. 2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej - w stosownym przypadku - o: a) celach przetwarzania lub kategorii przetwarzania; b) kategoriach danych osobowych; c) zakresie wprowadzonych ograniczeń; d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu; e) określeniu administratora lub kategorii administratorów; f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania; g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz h) prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.
Art. 6 pkt 2 Przepisów ustawy oraz rozporządzenia nr 2016/679 nie stosuje się do: działalności służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.	Artykuł 2 Materialny zakres stosowania 1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych 2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych: a) w ramach działalności nieobjętej zakresem prawa Unii; b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE; c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze; d) 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. Motyw 16 Niniejsze rozporządzenie nie ma zastosowania do kwestii ochrony podstawowych praw i wolności ani do swobodnego przepływu danych osobowych w związku z działalnością nieobjętą zakresem prawa Unii, taką jak działalność dotycząca bezpieczeństwa

	narodowego. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez państwa członkowskie w związku z działaniami związanymi ze wspólną polityką zagraniczną i bezpieczeństwa Unii.
Art. 97. Ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2017 r. poz. 1369, 1370 i 2451), wiążą sąd w postępowaniu o naprawnienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów.	Artykuł 79 Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu 1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia. Artykuł 82 Prawo do odszkodowania i odpowiedzialność 1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. 2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. 3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. 4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. 5. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą

	wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2. 6. Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2.

Projekt

USTAWA

z dnia

o ochronie danych osobowych[1), 2), 3)]

---

1) Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

3) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, ustawę z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, ustawę z dnia 31 lipca 1981 r. o wynagradzaniu niektórych osób zajmujących kierownicze stanowiska państwowe, ustawę z dnia 16 września 1982 r. o pracownikach urzędów państwowych, ustawę z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, ustawę z dnia 29 czerwca 1995 r. o statystyce publicznej, ustawę z dnia 10 kwietnia 1997 r. – Prawo energetyczne, ustawę z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, ustawę z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawę z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, ustawę z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów, ustawę z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, ustawę z dnia 28 listopada 2003 r. o świadczeniach rodzinnych, ustawę z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, ustawę z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, ustawę z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym, ustawę z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów, ustawę z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów, ustawę z dnia 27 sierpnia 2009 r. o finansach publicznych, ustawę z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, ustawę z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, ustawę z dnia 9 kwietnia 2010 r. o Służbie Więziennej, ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, ustawę z dnia 5 stycznia 2011 r. – Kodeks wyborczy, ustawę z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej, ustawę z dnia 19 sierpnia 2011 r. o usługach płatniczych, ustawę z dnia 14 grudnia 2012 r. o odpadach, ustawę z dnia 20 lutego 2015 r. o odnawialnych źródłach energii, ustawę z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach, ustawę z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, ustawę z dnia 25 września 2015 r. o zawodzie fizjoterapeuty, ustawę z dnia 9 października 2015 r. o produktach biobójczych, ustawę z dnia 28 stycznia 2016 r. – Prawo o prokuraturze, ustawę z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci, ustawę z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego, ustawę z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych, ustawę z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej, ustawę z dnia 9 marca 2017 r. o systemie monitorowania drogowego przewozu towarów oraz ustawę z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej. Niniejszą ustawą uchyla się ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679".

2. Ustawa określa:

1) podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu;
2) warunki i tryb akredytacji podmiotu certyfikującego, podmiotu monitorującego kodeks postępowania oraz certyfikacji;
3) tryb zatwierdzenia kodeksu postępowania;
4) organ właściwy w sprawie ochrony danych osobowych;
5) postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;
6) tryb europejskiej współpracy administracyjnej;
7) kontrolę przestrzegania przepisów o ochronie danych osobowych;
8) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem;
9) odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

Art. 2. 1. Do działalności polegającej na redagowaniu, przygotowaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. poz. 24, z późn. zm.[4)]), a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5–9, art. 11, art. 13–16, art. 18–22, art. 27, art. 28 ust. 2–10 oraz art. 30 rozporządzenia 2016/679.

[4)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1988 r. poz. 324, z 1989 r. poz. 187, z 1990 r. poz. 173, z 1991 r. poz. 442, z 1996 r. poz. 542, z 1997 r. poz. 554 i 770, z 1999 r. poz. 999, z 2001 r. poz. 1198, z 2002 r. poz. 1271, z 2004 r. poz. 1181, z 2005 r. poz. 377, z 2007 r. poz. 590, z 2010 r. poz. 1228 i 1551, z 2011 r. poz. 459, 934, 1204 i 1660, z 2012 r. poz. 1136, z 2013 r. poz. 771 oraz z 2017 r. poz. 2173.

2. Do wypowiedzi akademickiej, o której mowa w art. 85 ust. 2 rozporządzenia 2016/679, nie stosuje się przepisów art. 13, art. 15 ust. 3 i 4, art. 18, art. 27, art. 28 ust. 2–10 oraz art. 30 rozporządzenia 2016/679.

Art. 3. 1. Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679, jeżeli zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 13 ust. 3 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji:

1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego, lub
2) naruszy ochronę informacji niejawnych.

2. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą.

3. Administrator jest obowiązany bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca, poinformować osobę, której dane dotyczą, na jej wniosek, o podstawie nieprzekazania informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679.

Art. 4. 1. W zakresie nieuregulowanym w art. 14 ust. 5 rozporządzenia 2016/679 administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji:

1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego, lub
2) naruszy ochronę informacji niejawnych.

2. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą.

3. Administrator jest obowiązany bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca, poinformować osobę, której dane dotyczą, na jej wniosek, o podstawie nieprzekazania informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679.

Art. 5. 1. Przepisów, o których mowa w art. 15 ust. 1–3 rozporządzenia 2016/679, nie stosuje się, w przypadku gdy osoba, której dane dotyczą, nie jest informowana na podstawie art. 4 ust. 1.

2. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 rozporządzenia 2016/679, wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, administrator wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Przepis art. 64 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149) stosuje się odpowiednio.

3. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą.

4. Administrator jest obowiązany bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca, poinformować osobę, której dane dotyczą, na jej wniosek, o podstawie nieprzekazania informacji, o których mowa w art. 15 ust. 1 i 3 rozporządzenia 2016/679.

Art. 6. Przepisów ustawy oraz rozporządzenia 2016/679 nie stosuje się do:

1) przetwarzania danych osobowych przez jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 3, 5, 6 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62), w zakresie, w jakim przetwarzanie to jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego, jeżeli przepisy szczególne przewidują niezbędne środki ochrony praw i wolności osoby, której dane dotyczą;
2) działalności służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2017 r. poz. 1920 i 2405 oraz z 2018 r. poz. 138).

Art. 7. 1. W sprawach nieuregulowanych w ustawie do postępowań administracyjnych przed Prezesem Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu", o których mowa w rozdziale 4–7 i 11, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

2. Postępowanie przed Prezesem Urzędu jest postępowaniem jednoinstancyjnym.

3. Do postanowień wydanych w postępowaniach, o których mowa w ust. 1, na które zgodnie z ustawą z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego przysługuje zażalenie, przepisów o zażaleniu nie stosuje się.

4. Na postanowienia, o których mowa w ust. 3, przysługuje skarga do sądu administracyjnego.

Rozdział 2

Wyznaczanie inspektora ochrony danych

Art. 8. Administrator i podmiot przetwarzający jest obowiązany do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem", w przypadkach i na zasadach określonych w art. 37 rozporządzenia 2016/679.

Art. 9. Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
2) instytuty badawcze, o których mowa w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2017 r. poz. 1158, 1452 i 2201);
3) Narodowy Bank Polski.

Art. 10. 1. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

2. Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, o którym mowa w ust. 1. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej.

3. W zawiadomieniu obok danych, o których mowa w ust. 1, wskazuje się:

1) imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna;
2) firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą;
3) pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 albo 2;

4) numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.

4. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

5. W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorstw, każdy z tych podmiotów dokonuje zawiadomienia, o którym mowa w ust. 1 i 4.

6. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Art. 11. Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Rozdział 3

Warunki i tryb udzielania akredytacji podmiotowi certyfikującemu

Art. 12. 1. Akredytacji podmiotów ubiegających się o uprawnienie do certyfikacji w zakresie ochrony danych osobowych, o której mowa w art. 43 rozporządzenia 2016/679, zwanej dalej „akredytacją", udziela Polskie Centrum Akredytacji.

2. Akredytacja jest udzielana na zasadach określonych w art. 43 ust. 1–7 rozporządzenia 2016/679.

3. Do udzielania akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398), z wyłączeniem art. 24 ust. 4–7 oraz art. 25 ust. 1 i 2, w zakresie dotyczącym ograniczenia zakresu akredytacji oraz jej zawieszenia.

4. Ilekroć w ustawie jest mowa o podmiocie certyfikującym, należy przez to rozumieć podmiot uprawniony do certyfikacji w zakresie ochrony danych osobowych, akredytowany przez Polskie Centrum Akredytacji.

Art. 13. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria akredytacji, o których mowa w art. 43 ust. 3 rozporządzenia 2016/679.

Art. 14. 1. Polskie Centrum Akredytacji informuje Prezesa Urzędu o udzielonej akredytacji. Informacja o udzielonej akredytacji zawiera:

1) oznaczenie podmiotu, któremu udzielono akredytacji;
2) wskazanie zakresu udzielonej akredytacji oraz okresu jej ważności.

2. Polskie Centrum Akredytacji informuje Prezesa Urzędu o cofnięciu akredytacji. Informacja o cofnięciu akredytacji zawiera:

1) oznaczenie podmiotu, któremu cofnięto akredytację;
2) wskazanie powodów uzasadniających cofnięcie akredytacji.

3. Prezes Urzędu i Polskie Centrum Akredytacji mogą zawrzeć porozumienie o współpracy w zakresie monitorowania działalności podmiotów certyfikujących i wzajemnym przekazywaniu informacji dotyczących tych podmiotów.

Rozdział 4

Warunki i tryb dokonywania certyfikacji

Art. 15. 1. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, zwanej dalej „certyfikacją", dokonuje Prezes Urzędu i podmiot certyfikujący, na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek.

2. Certyfikacja jest dokonywana na zasadach określonych w rozporządzeniu 2016/679.

3. W sprawach dokonywania certyfikacji przez podmiot certyfikujący nieuregulowanych w rozporządzeniu 2016/679 i niniejszej ustawie stosuje się postanowienia umowy cywilnoprawnej zawartej między podmiotem certyfikującym a podmiotem ubiegającym się o certyfikację.

Art. 16. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679.

Art. 17. 1. Wniosek o certyfikację zawiera co najmniej:

1) nazwę podmiotu ubiegającego się o certyfikację albo jego imię i nazwisko oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania;
2) informacje potwierdzające spełnianie kryteriów certyfikacji;
3) wskazanie zakresu wnioskowanej certyfikacji.

2. Do wniosku dołącza się dokumenty potwierdzające spełnianie kryteriów certyfikacji albo ich kopie oraz, w przypadku certyfikacji dokonywanej przez Prezesa Urzędu, dowód wniesienia opłaty, o której mowa w art. 26.

3. Wniosek składa się pisemnie w postaci papierowej opatrzonej własnoręcznym podpisem albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym. Wniosek składany do Prezesa Urzędu w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Art. 18. 1. Prezes Urzędu albo podmiot certyfikujący rozpatruje wniosek o certyfikację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia wniosku zgodnego z art. 17, po zbadaniu spełniania kryteriów certyfikacji, zawiadamia wnioskodawcę o dokonaniu albo odmowie dokonania certyfikacji.

2. Wniosek złożony do Prezesa Urzędu, niezawierający informacji, o których mowa w art. 17 ust. 1 pkt 1, pozostawia się bez rozpoznania. Jeżeli wniosek nie zawiera informacji, o których mowa w art. 17 ust. 1 pkt 2 lub 3, lub nie spełnia wymagań, o których mowa w art. 17 ust. 2 lub 3, Prezes Urzędu wzywa wnioskodawcę do ich uzupełnienia wraz z pouczeniem, że ich nieuzupełnienie w terminie 7 dni od dnia doręczenia wezwania spowoduje pozostawienie wniosku bez rozpoznania.

Art. 19. Przed dokonaniem certyfikacji podmiot certyfikujący informuje Prezesa Urzędu o planowanym dokonaniu albo planowanej odmowie dokonania certyfikacji.

Art. 20. 1. W przypadku stwierdzenia, że podmiot ubiegający się o certyfikację nie spełnia kryteriów certyfikacji, Prezes Urzędu albo podmiot certyfikujący odmawia jej dokonania.

2. Odmowa dokonania certyfikacji przez Prezesa Urzędu następuje w drodze decyzji.

3. Podmiot certyfikujący opracowuje i udostępnia zainteresowanym podmiotom procedurę postępowania w przypadku odmowy dokonania certyfikacji.

Art. 21. 1. Dokumentem potwierdzającym certyfikację jest certyfikat.

2. Certyfikat zawiera co najmniej:

1) oznaczenie podmiotu, który otrzymał certyfikat;
2) nazwę podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby;
3) numer lub oznaczenie certyfikatu;
4) zakres, w tym okres, certyfikacji;

5) datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej.

Art. 22. 1. W okresie, na jaki została dokonana certyfikacja, podmiot, któremu wydano certyfikat, jest obowiązany spełniać kryteria certyfikacji obowiązujące na dzień jego wydania.

2. Prezes Urzędu albo podmiot certyfikujący cofa certyfikację w przypadku stwierdzenia, że podmiot, któremu wydano certyfikat, nie spełnia lub przestał spełniać kryteria certyfikacji.

3. Cofnięcie certyfikacji przez Prezesa Urzędu następuje w drodze decyzji.

Art. 23. 1. Podmiot certyfikujący przekazuje Prezesowi Urzędu dane podmiotu, któremu wydano certyfikat, oraz podmiotu, któremu cofnięto certyfikację, wraz ze wskazaniem przyczyny jej cofnięcia.

2. Prezes Urzędu prowadzi publicznie dostępny wykaz podmiotów, o których mowa w ust. 1.

3. Prezes Urzędu dokonuje wpisu do wykazu niezwłocznie po dokonaniu certyfikacji albo otrzymaniu informacji o dokonaniu certyfikacji przez podmiot certyfikujący.

4. Prezes Urzędu udostępnia wykaz na swojej stronie podmiotowej Biuletynu Informacji Publicznej i dokonuje jego aktualizacji.

Art. 24. 1. Prezes Urzędu w terminie, o którym mowa w art. 18 ust. 1, a także po dokonaniu certyfikacji jest uprawniony do przeprowadzenia czynności sprawdzających u administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek, w celu oceny spełniania przez ten podmiot kryteriów certyfikacji.

2. Prezes Urzędu zawiadamia podmiot, o którym mowa w ust. 1, o zamiarze przeprowadzenia czynności sprawdzających.

3. Czynności sprawdzające przeprowadza się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia podmiotowi, o którym mowa w ust. 1, zawiadomienia o zamiarze ich przeprowadzenia. Jeżeli czynności sprawdzające nie zostaną przeprowadzone w terminie 30 dni od dnia doręczenia zawiadomienia, ich przeprowadzenie wymaga ponownego zawiadomienia.

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

1) imię i nazwisko osoby przeprowadzającej czynności sprawdzające;

2) oznaczenie administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek;
3) wskazanie podstawy prawnej przeprowadzenia czynności sprawdzających;
4) zakres czynności sprawdzających;
5) datę i miejsce jego wystawienia;
6) podpis osoby uprawnionej do wydania upoważnienia w imieniu Prezesa Urzędu.

Art. 25. 1. Osoba przeprowadzająca czynności sprawdzające jest uprawniona do:
1) wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń w dniach i godzinach pracy administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek;
2) wglądu do dokumentów i informacji mających bezpośredni związek z działalnością objętą certyfikacją;
3) oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
4) żądania ustnych lub pisemnych wyjaśnień w sprawach związanych z działalnością objętą certyfikacją.

2. Czynności sprawdzających dokonuje się w obecności administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek lub osoby przez niego upoważnionej.

3. Z czynności sprawdzających sporządza się protokół i przedstawia administratorowi, podmiotowi przetwarzającemu, producentowi albo podmiotowi wprowadzającemu usługę lub produkt na rynek. Przepis art. 88 stosuje się odpowiednio.

Art. 26. 1. Prezes Urzędu pobiera za czynności związane z certyfikacją opłatę, której wysokość odpowiada przewidywanym kosztom poniesionym z tytułu wykonywania tych czynności.

2. Prezes Urzędu, ustalając wysokość opłaty, bierze pod uwagę zakres certyfikacji, przewidywany przebieg i długość postępowania certyfikującego oraz koszt pracy pracownika wykonującego czynności związane z certyfikacją.

3. Maksymalna wysokość opłaty nie może przekroczyć czterokrotności przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok złożenia wniosku o certyfikację, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r.

o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2017 r. poz. 1383, 1386 i 2120 oraz z 2018 r. poz. 138 i 357).

4. Prezes Urzędu na swojej stronie podmiotowej Biuletynu Informacji Publicznej podaje wysokość opłaty, którą podmiot, o którym mowa w art. 15, obowiązany jest ponieść z tytułu czynności związanych z certyfikacją.

5. Opłata stanowi dochód budżetu państwa.

Rozdział 5

Opracowywanie i zatwierdzanie kodeksu postępowania oraz warunki i tryb akredytacji podmiotu monitorującego jego przestrzeganie

Art. 27. 1. Kodeks postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, zwany dalej „kodeksem postępowania", jest opracowywany, opiniowany i zatwierdzany na zasadach określonych w tym rozporządzeniu.

2. Kodeks postępowania przed przekazaniem do zatwierdzenia Prezesowi Urzędu podlega konsultacjom z zainteresowanymi podmiotami.

3. Informację o przeprowadzonych konsultacjach oraz ich wyniku przekazuje się Prezesowi Urzędu wraz z kodeksem postępowania.

4. W przypadku uznania przez Prezesa Urzędu zakresu konsultacji za niewystarczający, wzywa on podmiot do przeprowadzenia ponownych konsultacji, wskazując ich zakres.

5. Stroną postępowania w sprawie zatwierdzenia kodeksu postępowania jest wyłącznie wnioskodawca występujący o zatwierdzenie tego kodeksu. Przepisu art. 31 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

6. Do zmiany zatwierdzonego kodeksu postępowania lub jego rozszerzenia stosuje się ust. 1–5.

Art. 28. Przestrzeganie zatwierdzonego kodeksu postępowania monitoruje podmiot akredytowany przez Prezesa Urzędu na zasadach określonych w art. 41 rozporządzenia 2016/679.

Art. 29. 1. Akredytacja podmiotu, o którym mowa w art. 28, jest udzielana na wniosek, który zawiera co najmniej:

1) nazwę podmiotu ubiegającego się o akredytację oraz adres jego siedziby;
2) informacje potwierdzające spełnianie kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679.

2. Do wniosku dołącza się dokumenty potwierdzające spełnianie kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, albo ich kopie.

3. Wniosek składa się pisemnie w postaci papierowej opatrzonej własnoręcznym podpisem albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Art. 30. 1. Prezes Urzędu rozpatruje wniosek i w terminie nie dłuższym niż 3 miesiące od dnia złożenia wniosku zgodnego z art. 29, po zbadaniu spełniania kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, zawiadamia podmiot ubiegający się o akredytację o udzieleniu lub odmowie udzielenia akredytacji.

2. Wniosek złożony do Prezesa Urzędu niezawierający informacji, o których mowa w art. 29 ust. 1 pkt 1, pozostawia się bez rozpoznania. Jeżeli wniosek nie zawiera informacji, o których mowa w art. 29 ust. 1 pkt 2, lub nie spełnia wymagań, o których mowa w ust. 2 lub 3, Prezes Urzędu wzywa wnioskodawcę do ich uzupełnienia wraz z pouczeniem, że ich nieuzupełnienie w terminie 7 dni od dnia doręczenia wezwania spowoduje pozostawienie wniosku bez rozpoznania.

3. W przypadku stwierdzenia, że podmiot ubiegający się o akredytację nie spełnia kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, odmawia udzielenia akredytacji. Odmowa udzielania akredytacji następuje w drodze decyzji.

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

2. Certyfikat akredytacyjny zawiera co najmniej:

1) oznaczenie podmiotu akredytowanego i adres jego siedziby;
2) numer lub oznaczenie certyfikatu akredytacyjnego;
3) datę wydania i podpis Prezesa Urzędu albo osoby przez niego upoważnionej.

Art. 32. 1. W okresie, na jaki akredytacja została udzielona, podmiot akredytowany jest obowiązany spełniać kryteria, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, obowiązujące na dzień wydania certyfikatu akredytacyjnego.

2. Prezes Urzędu cofa, w drodze decyzji, akredytację w przypadku stwierdzenia, że podmiot akredytowany:

1) nie spełnia lub przestał spełniać kryteria akredytacji, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679;
2) podejmuje działania niezgodne z przepisami rozporządzenia 2016/679.

Art. 33. 1. Prezes Urzędu prowadzi publicznie dostępny wykaz podmiotów akredytowanych.

2. Prezes Urzędu dokonuje wpisu do wykazu niezwłocznie po udzielaniu akredytacji.

3. Prezes Urzędu udostępnia wykaz na swojej stronie podmiotowej Biuletynu Informacji Publicznej i dokonuje jego aktualizacji.

Rozdział 6

Prezes Urzędu Ochrony Danych Osobowych

Art. 34. 1. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych.

2. Prezes Urzędu jest organem nadzorczym w rozumieniu rozporządzenia 2016/679, w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89) oraz w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującego i uchylającego decyzję Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz. Urz. UE L 135 z 24.05.2016, str. 53).

3. Prezesa Urzędu powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu Rzeczypospolitej Polskiej.

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

1) jest obywatelem polskim;
2) posiada wyższe wykształcenie;
3) wyróżnia się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych;
4) korzysta z pełni praw publicznych;
5) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
6) posiada nieposzlakowaną opinię.

5. Prezes Urzędu w zakresie wykonywania swoich zadań podlega tylko ustawie.

6. Kadencja Prezesa Urzędu trwa 4 lata, licząc od dnia złożenia ślubowania. Prezes Urzędu po upływie kadencji wykonuje swoje obowiązki do czasu objęcia stanowiska przez nowego Prezesa Urzędu.

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

8. Kadencja Prezesa Urzędu wygasa z chwilą jego śmierci, odwołania lub utraty obywatelstwa polskiego.

9. Prezes Urzędu może zostać odwołany przed upływem kadencji, wyłącznie w przypadku, gdy:

1) zrzekł się stanowiska;
2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby stwierdzonej orzeczeniem lekarskim;
3) sprzeniewierzył się ślubowaniu;
4) został skazany prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego;
5) został pozbawiony praw publicznych.

10. W przypadku odwołania lub wygaśnięcia kadencji Prezesa Urzędu jego obowiązki pełni zastępca Prezesa Urzędu wskazany przez Marszałka Sejmu.

Art. 35. 1. Przed przystąpieniem do wykonywania obowiązków Prezes Urzędu składa przed Sejmem Rzeczypospolitej Polskiej ślubowanie o następującej treści:

„Obejmując stanowisko Prezesa Urzędu Ochrony Danych Osobowych, uroczyście ślubuję dochować wierności postanowieniom Konstytucji Rzeczypospolitej Polskiej, strzec prawa do ochrony danych osobowych, a powierzone mi obowiązki wypełniać sumiennie i bezstronnie.”.

2. Ślubowanie może zostać złożone z dodaniem słów „Tak mi dopomóż Bóg”.

Art. 36. 1. Prezes Urzędu może powołać do trzech zastępców.

2. Na zastępcę Prezesa Urzędu może być powołana osoba, która:

1) jest obywatelem polskim;
2) posiada wyższe wykształcenie;
3) wyróżnia się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych;
4) korzysta z pełni praw publicznych;

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

6) posiada nieposzlakowaną opinię.

Art. 37. 1. Prezes Urzędu oraz jego zastępcy nie mogą zajmować innego stanowiska, z wyjątkiem stanowiska dydaktycznego, naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, ani wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu.

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

Art. 38. 1. Prezes Urzędu nie może być bez uprzedniej zgody Sejmu Rzeczypospolitej Polskiej pociągnięty do odpowiedzialności karnej ani pozbawiony wolności, z zastrzeżeniem ust. 2.

2. Prezes Urzędu może wyrazić zgodę na pociągnięcie go do odpowiedzialności karnej za wykroczenia, o których mowa w ust. 3, w trybie określonym w tym przepisie.

3. W przypadku popełnienia przez Prezesa Urzędu wykroczenia, o którym mowa w rozdziale XI ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz. U. z 2018 r. poz. 618), przyjęcie przez Prezesa Urzędu mandatu karnego albo uiszczenie grzywny, w przypadku ukarania mandatem karnym zaocznym, o którym mowa w art. 98 § 1 pkt 3 ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475), stanowi oświadczenie o wyrażeniu przez niego zgody na pociągniecie go do odpowiedzialności w tej formie.

4. Prezes Urzędu nie może być zatrzymany lub aresztowany, z wyjątkiem ujęcia go na gorącym uczynku przestępstwa i jeżeli jego zatrzymanie jest niezbędne do zapewnienia prawidłowego toku postępowania. O zatrzymaniu niezwłocznie powiadamia się Marszałka Sejmu, który może nakazać natychmiastowe zwolnienie zatrzymanego.

Art. 39. Przedawnienie w postępowaniu karnym czynu objętego immunitetem nie biegnie w okresie korzystania z immunitetu.

Art. 40. 1. Wniosek o wyrażenie zgody na pociągniecie Prezesa Urzędu do odpowiedzialności karnej w sprawie o przestępstwo ścigane z oskarżenia publicznego składa się za pośrednictwem Prokuratora Generalnego.

2. Wniosek o wyrażenie zgody na pociągniecie Prezesa Urzędu do odpowiedzialności karnej w sprawie o przestępstwo ścigane z oskarżenia prywatnego składa oskarżyciel prywatny, po wniesieniu sprawy do sądu.

3. Wniosek, o którym mowa w ust. 2, sporządza i podpisuje adwokat lub radca prawny, z wyjątkiem wniosków składanych w swoich sprawach przez sędziów, prokuratorów, adwokatów, radców prawnych, notariuszy oraz profesorów i doktorów habilitowanych nauk prawnych.

4. Wnioski, o których mowa w ust. 1 i 2, powinny zawierać:

1) oznaczenie wnioskodawcy oraz pełnomocnika, o ile został ustanowiony;
2) imię i nazwisko oraz datę i miejsce urodzenia Prezesa Urzędu;
3) wskazanie podstawy prawnej wniosku;
4) dokładne określenie czynu, którego dotyczy wniosek, ze wskazaniem czasu, miejsca, sposobu i okoliczności jego popełnienia oraz skutków, a zwłaszcza charakteru powstałej szkody;
5) uzasadnienie.

Art. 41. 1. Wniosek o wyrażenie zgody na pociągniecie Prezesa Urzędu do odpowiedzialności karnej składa się Marszałkowi Sejmu.

2. Jeżeli wniosek nie spełnia wymogów formalnych, o których mowa w art. 40 ust. 3 lub 4, Marszałek Sejmu wzywa wnioskodawcę do poprawienia lub uzupełnienia wniosku w terminie 14 dni, wskazując niezbędny zakres poprawienia lub uzupełnienia. W przypadku niepoprawienia lub nieuzupełnienia wniosku we wskazanym terminie i zakresie Marszałek Sejmu postanawia o pozostawieniu wniosku bez biegu.

3. Jeżeli wniosek spełnia wymogi formalne, o których mowa w art. 40 ust. 3 i 4, Marszałek Sejmu kieruje go do organu właściwego na podstawie Regulaminu Sejmu do rozpatrzenia wniosku, zawiadamiając jednocześnie Prezesa Urzędu o treści wniosku.

4. Organ właściwy do rozpatrzenia wniosku powiadamia Prezesa Urzędu o terminie jego rozpatrzenia. Między doręczeniem powiadomienia a terminem rozpatrzenia wniosku, o ile nie zachodzi wypadek niecierpiący zwłoki, powinno upłynąć co najmniej 7 dni.

5. Na żądanie organu właściwego do rozpatrzenia wniosku sąd albo odpowiedni organ, przed którym toczy się postępowanie wobec Prezesa Urzędu, udostępnia akta postępowania.

6. Prezes Urzędu przedstawia organowi właściwemu do rozpatrzenia wniosku wyjaśnienia i własne wnioski w tej sprawie w formie pisemnej lub ustnej.

7. Po rozpatrzeniu sprawy organ właściwy do rozpatrzenia wniosku uchwala sprawozdanie wraz z propozycją przyjęcia lub odrzucenia wniosku.

8. W trakcie rozpatrywania przez Sejm Rzeczypospolitej Polskiej sprawozdania, o którym mowa w ust. 7, Prezesowi Urzędu przysługuje prawo zabrania głosu.

9. Sejm Rzeczypospolitej Polskiej wyraża zgodę na pociągnięcie Prezesa Urzędu do odpowiedzialności karnej w drodze uchwały podjętej bezwzględną większością ustawowej liczby posłów. Nieuzyskanie wymaganej większości głosów oznacza podjęcie uchwały o niewyrażeniu zgody na pociągnięcie Prezesa Urzędu do odpowiedzialności karnej.

Art. 42. 1. Zakaz zatrzymania, o którym mowa w art. 38 ust. 4, obejmuje wszelkie formy pozbawienia lub ograniczenia wolności osobistej Prezesa Urzędu przez organy uprawnione do stosowania środków przymusu.

2. Wniosek o wyrażenie zgody na zatrzymanie lub aresztowanie Prezesa Urzędu składa się za pośrednictwem Prokuratora Generalnego.

3. Wniosek, o którym mowa w ust. 2, powinien zawierać:

1) oznaczenie wnioskodawcy;
2) imię i nazwisko oraz datę i miejsce urodzenia Prezesa Urzędu;
3) dokładne określenie czynu oraz jego kwalifikację prawną;
4) podstawę prawną zastosowania określonego środka;
5) uzasadnienie, wskazujące w szczególności na konieczność zastosowania określonego środka.

4. Do postępowania z wnioskiem o wyrażenie zgody na zatrzymanie lub aresztowanie Prezesa Urzędu przepisy art. 41 ust. 1–8 stosuje się odpowiednio.

5. Sejm Rzeczypospolitej Polskiej wyraża zgodę na zatrzymanie lub aresztowanie Prezesa Urzędu w drodze uchwały podjętej bezwzględną większością ustawowej liczby posłów. Nieuzyskanie wymaganej większości głosów oznacza podjęcie uchwały o niewyrażeniu zgody na zatrzymanie lub aresztowanie Prezesa Urzędu.

6. Wymóg uzyskania zgody Sejmu Rzeczypospolitej Polskiej nie dotyczy wykonania kary pozbawienia wolności orzeczonej prawomocnym wyrokiem sądu.

Art. 43. 1. Marszałek Sejmu przesyła wnioskodawcy niezwłocznie uchwałę, o której mowa w art. 41 ust. 9 i art. 42 ust. 5.

2. Uchwały, o których mowa w ust. 1, podlegają ogłoszeniu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

Art. 44. Przepisy ustawy dotyczące odpowiedzialności karnej Prezesa Urzędu stosuje się odpowiednio do odpowiedzialności za wykroczenia.

Art. 45. Szczegółowy tryb postępowania w sprawach, o których mowa w art. 39–44, określa Regulamin Sejmu.

Art. 46. 1. Prezes Urzędu wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych, zwanego dalej „Urzędem".

2. W przypadkach uzasadnionych charakterem i liczbą spraw z zakresu ochrony danych osobowych na danym terenie Prezes Urzędu może w ramach Urzędu tworzyć jednostki zamiejscowe Urzędu.

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

1) organizację wewnętrzną Urzędu,
2) zakres zadań swoich zastępców,
3) zakres zadań i tryb pracy komórek organizacyjnych Urzędu

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

Art. 47. 1. Prezes Urzędu, zastępcy Prezesa Urzędu, a także pracownicy Urzędu są obowiązani zachować w tajemnicy informacje, o których dowiedzieli się w związku z wykonywaniem czynności służbowych.

2. Obowiązek zachowania w tajemnicy informacji, o których mowa w ust. 1, nie może być ograniczony w czasie i trwa także po zakończeniu kadencji albo zatrudnienia.

Art. 48. Rada Ministrów określi, w drodze rozporządzenia, wzór legitymacji służbowej pracownika Urzędu, mając na względzie potrzebę zapewnienia możliwości identyfikacji osób uprawnionych do przeprowadzenia kontroli oraz wykonywania innych czynności służbowych.

Art. 49. 1. Przy Prezesie Urzędu działa Rada do Spraw Ochrony Danych Osobowych, zwana dalej „Radą", która jest organem opiniodawczo-doradczym Prezesa Urzędu.

2. Do zadań Rady należy:

1) opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych;
2) opiniowanie przekazanych przez Prezesa Urzędu projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych;

3) opracowywanie propozycji kryteriów certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679;
4) opracowywanie propozycji rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych;
5) inicjowanie działań w obszarze ochrony danych osobowych oraz przedstawianie Prezesowi Urzędu propozycji zmian prawa w tym obszarze;
6) wyrażanie opinii w sprawach przedstawionych Radzie przez Prezesa Urzędu;
7) wykonywanie innych zadań zleconych przez Prezesa Urzędu.

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

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

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

6. Rada składa się z 8 członków.

7. Kandydatów na członków Rady zgłasza:

1) Rada Ministrów;
2) Rzecznik Praw Obywatelskich;
3) izby gospodarcze;
4) jednostki naukowe w rozumieniu przepisów ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (Dz. U. z 2018 r. poz. 87);
5) fundacje i stowarzyszenia wpisane do Krajowego Rejestru Sądowego, których celem statutowym jest działalność na rzecz ochrony danych osobowych.

8. Członkiem Rady może być osoba, która:

1) posiada wykształcenie wyższe;
2) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
3) korzysta z pełni praw publicznych;
4) wyraziła zgodę na kandydowanie.

9. Członek Rady jest obowiązany do zachowania w tajemnicy informacji, o których dowiedział się w związku z wykonywaniem funkcji członka Rady. Prezes Urzędu może zwolnić z obowiązku zachowania tajemnicy w zakresie przez niego określonym.

10. Prezes Urzędu powołuje skład Rady, na dwuletnią kadencję, spośród kandydatów zgłoszonych przez podmioty, o których mowa w ust. 7, w tym 5 członków spośród kandydatów zgłoszonych przez podmioty, o których mowa w ust. 7 pkt 1 i 2, oraz 3 członków spośród kandydatów zgłoszonych przez podmioty, o których mowa w ust. 7 pkt 3–5.

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

1) rezygnacji członka Rady złożonej na piśmie przewodniczącemu Rady;
2) śmierci członka Rady;
3) niemożności sprawowania funkcji członka Rady z powodu długotrwałej choroby stwierdzonej zaświadczeniem lekarskim;
4) skazania prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) pozbawienia praw publicznych.

12. W przypadku, o którym mowa w ust. 11, Prezes Urzędu powołuje nowego członka Rady na okres pozostały do końca kadencji, spośród pozostałych zgłoszonych kandydatów, po potwierdzeniu aktualności zgłoszenia, z uwzględnieniem ust. 10.

13. Prezes Urzędu powołuje i odwołuje przewodniczącego Rady i wiceprzewodniczącego Rady spośród jej członków.

14. Przewodniczący Rady kieruje jej pracami i reprezentuje ją na zewnątrz. W przypadku nieobecności przewodniczącego Rady zastępuje go wiceprzewodniczący Rady.

15. Obsługę Rady zapewnia Urząd.

16. Na posiedzenie Rady mogą być zapraszane, przez Prezesa Urzędu oraz przewodniczącego Rady, inne osoby, o ile jest to uzasadnione zadaniami Rady. Przepis ust. 9 stosuje się odpowiednio.

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

Art. 50. 1. Za udział w pracach Rady członkowi przysługuje wynagrodzenie. Wysokość wynagrodzenia uzależniona jest od zakresu obowiązków związanych z funkcją pełnioną w Radzie oraz liczby posiedzeń, w których uczestniczył.

2. Wynagrodzenie członka Rady za jedno posiedzenie stanowi co najmniej 5% przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok powołania Rady, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r.

o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, i nie może przekroczyć 25% tego wynagrodzenia.

3. Rada Ministrów określi, w drodze rozporządzenia, wysokość wynagrodzenia członka Rady za udział w posiedzeniu oraz liczbę posiedzeń Rady w ciągu roku kalendarzowego, uwzględniając zakres obowiązków związanych z funkcją pełnioną w Radzie oraz prawidłową realizację zadań Rady.

4. Członkom Rady posiadającym miejsce zamieszkania poza siedzibą Prezesa Urzędu przysługują diety oraz zwrot kosztów podróży i zakwaterowania na warunkach określonych w przepisach wydanych na podstawie art. 77^5 § 2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 108, 138, 305 i 357).

Art. 51. 1. Prezes Urzędu raz w roku do dnia 31 sierpnia przedstawia Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności, zawierające w szczególności informację o liczbie i rodzaju prawomocnych orzeczeń sądowych uwzględniających skargi na decyzje lub postanowienia Prezesa Urzędu oraz wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych.

2. Prezes Urzędu udostępnia sprawozdanie, o którym mowa w ust. 1, na swojej stronie podmiotowej Biuletynu Informacji Publicznej.

Art. 52. Założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu.

Art. 53. 1. Prezes Urzędu może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych.

2. Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

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

Art. 54. 1. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej:

1) standardowe klauzule umowne, o których mowa w art. 28 ust. 8 rozporządzenia 2016/679;
2) zatwierdzone kodeksy postępowania, o których mowa w art. 40 rozporządzenia 2016/679, a także zmiany tych kodeksów;
3) przyjęte standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit. d rozporządzenia 2016/679;
4) rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.

2. Rekomendacje, o których mowa w ust. 1 pkt 4, sporządzane są z uwzględnieniem specyfiki danego rodzaju działalności i podlegają okresowej aktualizacji.

3. Projekt rekomendacji, o których mowa w ust. 1 pkt 4, Prezes Urzędu konsultuje z zainteresowanymi podmiotami, których zakresu działania dotyczy dany projekt.

Art. 55. 1. Prezes Urzędu:

1) ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679;
2) może ogłosić w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych niewymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 5 rozporządzenia 2016/679.

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

Art. 56. Prezes Urzędu może prowadzić system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679.

Art. 57. Prezes Urzędu, w drodze decyzji:

1) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 rozporządzenia 2016/679;
2) udziela zezwolenia, o którym mowa w art. 46 ust. 3 rozporządzenia 2016/679.

Art. 58. 1. Administrator danych lub podmiot przetwarzający może wystąpić do Prezesa Urzędu z wnioskiem o przeprowadzenie uprzednich konsultacji, o którym mowa w art. 36 rozporządzenia 2016/679.

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

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

Art. 59. Jeżeli Prezes Urzędu, na podstawie posiadanych informacji, uzna, że doszło do naruszenia przepisów dotyczących przetwarzania danych osobowych, może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom, które dopuściły się naruszeń, i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

Rozdział 7

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

Art. 60. Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", jest prowadzone przez Prezesa Urzędu.

Art. 61. Organizacja społeczna, o której mowa w art. 31 § 1 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, może również występować w postępowaniu za zgodą osoby, której dane dotyczą, w jej imieniu i na jej rzecz.

Art. 62. W przypadku, o którym mowa w art. 36 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, Prezes Urzędu, zawiadamiając strony o niezałatwieniu sprawy w terminie, jest obowiązany również poinformować o stanie sprawy i przeprowadzonych w jej toku czynnościach.

Art. 63. Prezes Urzędu może żądać od strony przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę. Tłumaczenie dokumentacji strona jest obowiązana wykonać na własny koszt.

Art. 64. W celu realizacji swoich zadań Prezes Urzędu ma prawo dostępu do informacji objętych tajemnicą prawnie chronioną, chyba że przepisy szczególne stanowią inaczej.

Art. 65. 1. Strona może zastrzec informacje, dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa, przedstawiane Prezesowi Urzędu. W takim przypadku strona jest obowiązana przedstawić Prezesowi Urzędu również wersję dokumentu niezawierającą informacji objętych zastrzeżeniem.

2. W przypadku nieprzedstawienia wersji dokumentu niezawierającej informacji objętych zastrzeżeniem, zastrzeżenie uważa się za nieskuteczne.

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

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

Art. 66. Prezes Urzędu wydaje postanowienie, o którym mowa w art. 74 § 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, również w przypadku, gdy udostępnienie tego materiału grozi ujawnieniem tajemnic prawnie chronionych albo ujawnieniem tajemnicy przedsiębiorstwa, jeżeli o ograniczenie wglądu do akt dla stron postępowania wnosi przedsiębiorca, od którego informacja pochodzi.

Art. 67. Jeżeli liczba stron w postępowaniu przekracza 20 osób, Prezes Urzędu może zastosować art. 49 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 68. 1. Jeżeli w toku postępowania zajdzie konieczność uzupełnienia dowodów, można przeprowadzić postępowanie kontrolne.

2. Okresu postępowania kontrolnego nie wlicza się do terminów, o których mowa w art. 35 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 69. 1. W przypadku, o którym mowa w art. 88 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, Prezes Urzędu wymierza karę grzywny w wysokości od 500 do 5000 zł.

2. Wymierzając karę grzywny, Prezes Urzędu bierze pod uwagę:

1) w przypadku osoby fizycznej, sytuację osobistą wezwanego i stopień zrozumienia powagi ciążących na nim obowiązków wynikających z wezwania, lub

2) potrzebę dostosowania wysokości grzywny do celu, jakim jest przymuszenie wezwanego do zadośćuczynienia wezwaniu.

3. Kara grzywny, o której mowa w ust. 1, może być nałożona także w przypadku, gdy strona odmówiła przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji.

Art. 70. 1. Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, Prezes Urzędu, w celu zapobieżenia tym skutkom, może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych, wskazując dopuszczalny zakres tego przetwarzania.

2. W postanowieniu, o którym mowa w ust. 1, Prezes Urzędu określa termin obowiązywania ograniczenia przetwarzania danych osobowych nie dłuższy niż do dnia wydania decyzji kończącej postępowanie w sprawie.

3. Na postanowienie przysługuje skarga do sądu administracyjnego.

Art. 71. 1. Jeżeli w toku postępowania Prezes Urzędu uzna, że istnieją uzasadnione wątpliwości co do zgodności z prawem Unii Europejskiej decyzji Komisji Europejskiej, o której mowa w art. 40 ust. 9 w sprawie kodeksu postępowania, o którym mowa w art. 46 ust. 2 lit. e, oraz decyzji, o której mowa w art. 45 i art. 46 ust. 2 lit. c rozporządzenia 2016/679, Prezes Urzędu występuje do sądu administracyjnego z wnioskiem o wystąpienie z pytaniem prawnym na podstawie art. 267 Traktatu o funkcjonowaniu Unii Europejskiej w sprawie ważności decyzji Komisji Europejskiej.

2. Wniosek poza spełnianiem wymagań dotyczących skargi, o których mowa w art. 64 § 2 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2017 r. poz. 1369, 1370 i 2451), zawiera w szczególności:

1) wskazanie decyzji Komisji Europejskiej, której wniosek dotyczy;
2) omówienie powodów, dla których organ powziął wątpliwości w kwestii ważności decyzji Komisji Europejskiej i jej niezgodności z przepisami prawa;

3) treść pytania lub pytań, które sąd administracyjny powinien przedstawić Trybunałowi Sprawiedliwości Unii Europejskiej, zawierającą:
   a) przedmiot sporu oraz ustalenia co do okoliczności faktycznych, w tym stanowisko strony podniesione w postępowaniu przed organem, jeżeli zostało przedstawione przez stronę,
   b) wskazanie przepisów prawa mających zastosowanie w sprawie,
   c) proponowaną do przedstawienia Trybunałowi Sprawiedliwości Unii Europejskiej przez sąd administracyjny sentencję pytania lub pytań;
4) oświadczenie o zgodności treści załącznika, o którym mowa w ust. 3, z wnioskiem złożonym w postaci papierowej.

3. Do wniosku dołącza się załącznik zawierający treść wniosku w formie dokumentu elektronicznego zapisanego na informatycznym nośniku danych w formacie danych pozwalającym na edycję jego treści (kopię).

4. Stroną postępowania przed sądem administracyjnym w sprawie wniosku jest Prezes Urzędu.

5. Sąd rozpoznaje wniosek na posiedzeniu niejawnym, w składzie 3 sędziów.

6. Sąd, uznając wniosek za uzasadniony, występuje do Trybunału Sprawiedliwości Unii Europejskiej z pytaniem prejudycjalnym na podstawie art. 267 Traktatu o funkcjonowaniu Unii Europejskiej.

7. W przypadku uznania przez sąd, że wniosek Prezesa Urzędu nie zawiera wystarczającego uzasadnienia dla wystąpienia z pytaniem prawnym do Trybunału Sprawiedliwości Unii Europejskiej, wydaje się postanowienie o odmowie wystąpienia z pytaniem.

8. Na postanowienie, o którym mowa w ust. 7, nie przysługuje środek odwoławczy.

9. Sąd sporządza uzasadnienie postanowienia w terminie 21 dni.

10. Od wniosku nie pobiera się opłaty sądowej.

Art. 72. W uzasadnieniu decyzji kończącej postępowanie w sprawie wskazuje się dodatkowo przesłanki określone w art. 83 ust. 2 rozporządzenia 2016/679, na których Prezes Urzędu oparł się, nakładając administracyjną karę pieniężną oraz ustalając jej wysokość.

Art. 73. 1. Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, po zakończeniu postępowania informuje o wydaniu decyzji na swojej stronie podmiotowej Biuletynu Informacji Publicznej.

2. Organy lub podmioty publiczne, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych oraz Narodowy Bank Polski, w stosunku do których Prezes Urzędu wydał prawomocną decyzję stwierdzającą naruszenie, niezwłocznie podają do publicznej wiadomości na swojej stronie internetowej lub stronie podmiotowej Biuletynu Informacji Publicznej, informację o działaniach podjętych w celu wykonania decyzji.

Art. 74. Wniesienie przez stronę skargi do sądu administracyjnego wstrzymuje wykonanie decyzji w zakresie administracyjnej kary pieniężnej.

Rozdział 8

Europejska współpraca administracyjna

Art. 75. 1. W przypadkach, o których mowa w art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 rozporządzenia 2016/679, Prezes Urzędu może wydać postanowienie o zastosowaniu środka tymczasowego, o którym mowa w art. 70 ust. 1.

2. W postanowieniu Prezes Urzędu określa termin obowiązywania środka tymczasowego, o którym mowa w art. 70 ust. 1, nie dłuższy niż 3 miesiące.

3. Na postanowienie przysługuje skarga do sądu administracyjnego.

Art. 76. Wszelkie informacje kierowane przez Prezesa Urzędu do organów nadzorczych innych państw członkowskich w ramach europejskiej współpracy administracyjnej podlegają tłumaczeniu na jeden z języków urzędowych tego państwa członkowskiego lub na język angielski.

Art. 77. W przypadku otrzymania przez Prezesa Urzędu wniosku organu nadzorczego innego państwa członkowskiego Unii Europejskiej dotyczącego uczestnictwa we wspólnej operacji, o której mowa w art. 62 ust. 1 rozporządzenia 2016/679, albo wystąpienia przez Prezesa Urzędu z takim wnioskiem, Prezes Urzędu dokonuje z organem nadzorczym innego państwa członkowskiego Unii Europejskiej ustaleń dotyczących wspólnej operacji i niezwłocznie sporządza wykaz ustaleń.

Rozdział 9

Kontrola przestrzegania przepisów o ochronie danych osobowych

Art. 78. 1. Prezes Urzędu przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych.

2. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa Urzędu informacji lub w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679.

Art. 79. 1. Kontrolę przeprowadza upoważniony przez Prezesa Urzędu:

1) pracownik Urzędu,

2) członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 rozporządzenia 2016/679

– zwany dalej „kontrolującym".

2. Kontrolujący, o którym mowa w ust. 1 pkt 2, jest obowiązany do zachowania w tajemnicy informacji, o których dowiedział się w toku kontroli.

Art. 80. 1. Kontrolujący podlega wyłączeniu z udziału w kontroli, na wniosek lub z urzędu, jeżeli:

1) wyniki kontroli mogłyby oddziaływać na prawa lub obowiązki jego, jego małżonka, osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnego i powinowatego do drugiego stopnia albo na osoby związanej z nim z tytułu przysposobienia, opieki albo kurateli;

2) zachodzą uzasadnione wątpliwości co do jego bezstronności.

2. Powody wyłączenia, o których mowa w ust. 1 pkt 1, trwają także po ustaniu małżeństwa, przysposobienia, opieki lub kurateli.

3. O przyczynach powodujących wyłączenie kontrolujący lub podmiot objęty kontrolą, zwany dalej „kontrolowanym", niezwłocznie zawiadamia Prezesa Urzędu.

4. O wyłączeniu kontrolującego rozstrzyga Prezes Urzędu.

5. Do czasu wydania postanowienia kontrolujący podejmuje czynności niecierpiące zwłoki.

Art. 81. 1. Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową, a w przypadku kontrolującego, o którym mowa w art. 79 ust. 1 pkt 2, członka lub pracownika organu nadzorczego państwa członkowskiego Unii Europejskiej, po okazaniu imiennego upoważnienia wraz z dokumentem potwierdzającym tożsamość.

2. Imienne upoważnienie do przeprowadzenia kontroli zawiera:

1) wskazanie podstawy prawnej przeprowadzenia kontroli;

2) oznaczenie organu;

3) imię i nazwisko, stanowisko służbowe kontrolującego oraz numer legitymacji służbowej, a w przypadku kontrolującego, o którym mowa w art. 79 ust. 1 pkt 2, imię i nazwisko oraz numer dokumentu potwierdzającego tożsamość;
4) określenie zakresu przedmiotowego kontroli;
5) oznaczenie kontrolowanego;
6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności kontrolnych;
7) podpis Prezesa Urzędu;
8) pouczenie kontrolowanego o jego prawach i obowiązkach;
9) datę i miejsce jego wystawienia.

Art. 82. 1. Prezes Urzędu może upoważnić do udziału w kontroli osobę posiadającą wiedzę specjalistyczną, jeżeli przeprowadzenie czynności kontrolnych wymaga takiej wiedzy. Przepis art. 80 i art. 81 ust. 2 stosuje się.

2. Zakres uprawnień osoby, o której mowa w ust. 1, jest określony w upoważnieniu udzielonym przez Prezesa Urzędu.

3. Osoba, o której mowa w ust. 1, jest obowiązana do zachowania w tajemnicy informacji, o których dowiedziała się w toku kontroli.

Art. 83. 1. Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej.

2. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli.

3. W razie nieobecności kontrolowanego lub osoby przez niego upoważnionej, upoważnienie do przeprowadzenia kontroli oraz legitymacja służbowa lub dokument potwierdzający tożsamość mogą być okazane:
1) osobie czynnej w lokalu przedsiębiorstwa w rozumieniu art. 97 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2017 r. poz. 459, 933 i 1132 oraz z 2018 r. poz. 398), lub
2) przywołanemu świadkowi, jeżeli jest funkcjonariuszem publicznym w rozumieniu art. 115 § 13 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204 oraz z 2018 r. poz. 20 i 305), niebędącemu pracownikiem Urzędu albo osobą, o której mowa w art. 80 ust. 1.

Art. 84. 1. Kontrolujący ma prawo:

1) wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń;
2) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
5) zlecać sporządzanie ekspertyz i opinii.

2. Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach, o których mowa w ust. 1 pkt 3.

3. Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 2. W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli.

4. W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub dźwięk. Informatyczne nośniki danych w rozumieniu przepisów o informatyzacji działalności podmiotów realizujących zadania publiczne, na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli.

Art. 85. 1. Prezes Urzędu lub kontrolujący może zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeżeli jest to niezbędne do przeprowadzenia czynności kontrolnych.

2. Komendant Policji udziela pomocy przy wykonywaniu czynności kontrolnych, po otrzymaniu pisemnego wezwania na co najmniej 7 dni przed terminem tych czynności.

3. W pilnych przypadkach, w szczególności gdy kontrolujący trafi na opór uniemożliwiający lub utrudniający przeprowadzenie czynności kontrolnych, udzielenie pomocy następuje również na ustne wezwanie Prezesa Urzędu lub kontrolującego, po

okazaniu upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej kontrolującego.

4. Prezes Urzędu przekazuje potwierdzenie wezwania na piśmie, nie później niż w terminie 3 dni po zakończeniu czynności kontrolnych.

5. Udzielenie pomocy Policji przy wykonywaniu kontroli polega na zapewnieniu kontrolującemu bezpieczeństwa osobistego oraz dostępu do miejsca wykonywania kontroli i porządku w tym miejscu.

6. Policja, udzielając pomocy kontrolującemu w kontroli, zapewnia bezpieczeństwo również innym osobom uczestniczącym w kontroli, mając w szczególności na względzie poszanowanie godności osób biorących udział w kontroli.

7. Koszty poniesione przez Policję z tytułu udzielonej pomocy przy wykonywaniu czynności kontrolnych rozlicza się według stawki zryczałtowanej w wysokości 1,5% przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich (Dz. U. z 2017 r. poz. 357).

Art. 86. 1. Kontrolujący może przesłuchać pracownika kontrolowanego w charakterze świadka.

2. Za pracownika kontrolowanego uznaje się osobę zatrudnioną na podstawie stosunku pracy oraz wykonującą pracę na podstawie umowy cywilnoprawnej.

3. Do przesłuchania pracownika kontrolowanego stosuje się art. 83 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 87. Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Art. 88. 1. Przebieg czynności kontrolnych kontrolujący przedstawia w protokole kontroli.

2. Protokół kontroli zawiera:

1) wskazanie nazwy albo imienia i nazwiska oraz adresu kontrolowanego;
2) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;

3) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia kontrolującego, a w przypadku kontrolującego, o którym mowa w art. 80 ust. 1 pkt 2, imię i nazwisko, numer dokumentu potwierdzającego tożsamość oraz numer upoważnienia;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie zakresu przedmiotowego kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) wyszczególnienie załączników;
8) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;
9) pouczenie kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu oraz o prawie odmowy podpisania protokołu;
10) datę i miejsce podpisania protokołu przez kontrolującego i kontrolowanego.

3. Protokół kontroli podpisuje kontrolujący i przekazuje kontrolowanemu w celu podpisania.

4. Kontrolowany w terminie 7 dni od dnia przedstawienia protokołu kontroli do podpisu, podpisuje go albo składa pisemne zastrzeżenia do jego treści.

5. W przypadku złożenia zastrzeżeń, kontrolujący dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu.

6. W razie nieuwzględnienia zastrzeżeń w całości lub w części, kontrolujący przekazuje kontrolowanemu informacje o tym wraz z uzasadnieniem.

7. Brak doręczenia kontrolującemu podpisanego protokołu i niezgłoszenie zastrzeżeń do treści protokołu w terminie, o którym mowa w ust. 4, uznaje się za odmowę podpisania protokołu.

8. O odmowie podpisania protokołu kontrolujący czyni wzmiankę w protokole, zawierającą datę jej dokonania. W przypadku, o którym mowa w ust. 7, wzmianki dokonuje się po upływie terminu, o którym mowa w ust. 4.

9. Protokół sporządza się w postaci elektronicznej albo w postaci papierowej w dwóch egzemplarzach. Protokół podlega doręczeniu kontrolowanemu.

Art. 89. 1. Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu lub podpisanie i doręczenie protokołu przez kontrolowanego.

2. Terminem zakończenia kontroli jest dzień podpisania protokołu kontroli przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 88 ust. 8.

Art. 90. Jeżeli na podstawie informacji zgromadzonych w postępowaniu kontrolnym Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania, o którym mowa w art. 60.

Art. 91. Przepisy art. 63–65 stosuje się odpowiednio.

Rozdział 10

Odpowiedzialność cywilna i postępowanie przed sądem

Art. 92. W zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny.

Art. 93. W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 rozporządzenia 2016/679, jest właściwy sąd okręgowy.

Art. 94. 1. O wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o którym mowa w art. 79 lub art. 82 rozporządzenia 2016/679, sąd zawiadamia niezwłocznie Prezesa Urzędu.

2. Prezes Urzędu zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona. Prezes Urzędu niezwłocznie informuje sąd również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia.

Art. 95. Sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed Prezesem Urzędu.

Art. 96. Sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, uwzględnia roszczenie dochodzone przed sądem.

Art. 97. Ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawnienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów.

Art. 98. 1. W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie w postępowaniu przed sądem, Prezes Urzędu może wytaczać powództwa na rzecz osoby, której dane dotyczą, za jej zgodą, a także wstępować, za zgodą powoda, do postępowania w każdym jego stadium.

2. W pozostałych sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych Prezes Urzędu może wstępować, za zgodą powoda, do postępowania przed sądem w każdym jego stadium, chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych.

3. W przypadkach, o których mowa w ust. 1 i 2, do Prezesa Urzędu stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 155, 398 i 416) o prokuratorze.

Art. 99. Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, przedstawia sądowi istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych.

Art. 100. Do postępowania w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 rozporządzenia 2016/679, w zakresie nieuregulowanym niniejszą ustawą stosuje się przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego.

Rozdział 11

Przepisy o administracyjnych karach pieniężnych i przepisy karne

Art. 101. Prezes Urzędu może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż:

1) jednostka sektora finansów publicznych w rozumieniu art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
2) instytut badawczy w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych,
3) Narodowy Bank Polski

– w drodze decyzji, administracyjną karę pieniężną na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

Art. 102. 1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
2) instytut badawczy w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych;
3) Narodowy Bank Polski.

2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

3. Administracyjne kary pieniężne, o których mowa w ust. 1 i 2, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

Art. 103. Równowartość wyrażonych w euro kwot, o których mowa w art. 83 rozporządzenia 2016/679, oblicza się w złotych według średniego kursu euro ogłoszonego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, a w przypadku gdy w danym roku Narodowy Bank Polski nie ogłasza średniego kursu euro w dniu 28 stycznia – według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów Narodowego Banku Polskiego.

Art. 104. Środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa.

Art. 105. 1. Administracyjną karę pieniężną uiszcza się w terminie 14 dni od dnia upływu terminu na wniesienie skargi, albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego.

2. Prezes Urzędu może, na wniosek podmiotu ukaranego, odroczyć uiszczenie administracyjnej kary pieniężnej albo rozłożyć ją na raty, ze względu na ważny interes wnioskodawcy.

3. Do wniosku dołącza się uzasadnienie.

4. W przypadku odroczenia uiszczenia administracyjnej kary pieniężnej albo rozłożenia jej na raty, Prezes Urzędu nalicza od nieuiszczonej kwoty odsetki w stosunku rocznym, przy zastosowaniu obniżonej stawki odsetek za zwłokę, ogłaszanej na podstawie art. 56d ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2017 r. poz. 201, z późn. zm.[5)]), od dnia następującego po dniu złożenia wniosku.

5. W przypadku rozłożenia administracyjnej kary pieniężnej na raty, odsetki, o których mowa w ust. 4, są naliczane odrębnie dla każdej raty.

6. W razie niedotrzymania odroczonego terminu płatności administracyjnej kary pieniężnej albo terminu zapłaty jej rat, odsetki są naliczane za okres od dnia upływu odroczonego terminu płatności kary albo terminu zapłaty poszczególnych rat.

7. Prezes Urzędu może uchylić odroczenie uiszczenia administracyjnej kary pieniężnej albo rozłożenie jej na raty, jeżeli ujawniły się nowe lub uprzednio nieznane okoliczności istotne dla rozstrzygnięcia lub jeżeli rata nie została uiszczona w terminie.

8. Rozstrzygnięcie Prezesa Urzędu w przedmiocie odroczenia uiszczenia administracyjnej kary pieniężnej albo rozłożenia jej na raty następuje w drodze postanowienia.

9. Prezes Urzędu, na wniosek podmiotu ukaranego prowadzącego działalność gospodarczą, może udzielić ulgi w wykonaniu administracyjnej kary pieniężnej określonej w ust. 2, która:

1) nie stanowi pomocy publicznej;
2) stanowi pomoc *de minimis* albo pomoc *de minimis* w rolnictwie lub rybołówstwie – w zakresie i na zasadach określonych w bezpośrednio obowiązujących przepisach prawa Unii Europejskiej dotyczących pomocy w ramach zasady *de minimis*;

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 648, 768, 935, 1428, 1537, 2169 i 2491 oraz z 2018 r. poz. 106, 138 i 398.

3) stanowi pomoc publiczną zgodną z zasadami rynku wewnętrznego Unii Europejskiej, której dopuszczalność została określona przez właściwe organy Unii Europejskiej.

Art. 106. Przepisów art. 189d–189f i art. 189k ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

Art. 107. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Art. 108. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Rozdział 12

Przepisy zmieniające

Art. 109. W ustawie z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 155, 398 i 416) w pkt 4^4 kropkę zastępuje się średnikiem i dodaje się pkt 4^5 w brzmieniu:

„4^5) o roszczenia wynikające z naruszenia praw przysługujących na mocy przepisów o ochronie danych osobowych.”.

Art. 110. W ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2017 r. poz. 1201, 1475, 1954 i 2491 oraz z 2018 r. poz. 138 i 398) wprowadza się następujące zmiany:

1) użyte w art. 2 w § 1 w pkt 12 i w art. 20 w § 2, w różnym przypadku wyrazy „Generalny Inspektor Ochrony Danych Osobowych” zastępuje się użytymi w odpowiednim przypadku wyrazami „Prezes Urzędu Ochrony Danych Osobowych”;
2) w art. 18i § 12 otrzymuje brzmienie:

„§ 12. Postępowanie w sprawie sprzeciwu nie wyłącza odpowiedzialności za naruszenie obowiązków wynikających z przepisów o ochronie danych osobowych.”.

Art. 111. W ustawie z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. z 2017 r. poz. 1998) użyte w art. 2 w pkt 2 i 4 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych” zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych”.

Art. 112. W ustawie z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. z 2017 r. poz. 2142 i 2203 oraz z 2018 r. poz. 106) użyte w art. 1 w ust. 1 w pkt 13, w art. 36 w ust. 5 w pkt 1 oraz w art. 48 w ust. 2, w różnym przypadku, wyrazy „Biuro Generalnego Inspektora Ochrony Danych Osobowych” zastępuje się użytymi w odpowiednim przypadku wyrazami „Urząd Ochrony Danych Osobowych”.

Art. 113. W ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524) wprowadza się następujące zmiany:

1) użyte w art. 4 w ust. 1 i 2 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych” zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych”;
2) w art. 29 w ust. 1 w pkt 2 lit. i otrzymuje brzmienie:
   „i) przetwarzania danych osobowych, z wyjątkiem danych ujawniających poglądy polityczne, przekonania religijne lub światopoglądowe, jak również danych genetycznych, o nałogach, o seksualności lub o orientacji seksualnej.”.

Art. 114. W ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2016 r. poz. 1068 oraz z 2017 r. poz. 60) użyte w art. 44 w ust. 2 w pkt 2 wyrazy „Generalnemu Inspektorowi Ochrony Danych Osobowych” zastępuje się wyrazami „Prezesowi Urzędu Ochrony Danych Osobowych”.

Art. 115. W ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2017 r. poz. 220, z późn. zm.[6)]) w art. 9c ust. 5a otrzymuje brzmienie:

„5a. Operatorzy systemów dystrybucyjnych instalujący u odbiorców końcowych przyłączonych do ich sieci liczniki zdalnego odczytu są obowiązani chronić dane pomiarowe dotyczące tych odbiorców na zasadach określonych w przepisach o ochronie danych osobowych.”.

[6)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 791, 1089, 1387 i 1566 oraz z 2018 r. poz. 9, 138 i 317.

Art. 116. W ustawie z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (Dz. U. z 2018 r. poz. 121 i 50) użyte w art. 60 w ust. 1 w pkt 1 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych" zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych".

Art. 117. W ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2018 r. poz. 511) w art. 6d ust. 4b otrzymuje brzmienie:

„4b. Podmioty wymienione w ust. 4a przetwarzają dane udostępnione z systemu w celu, w którym te dane zostały im udostępnione, na zasadach określonych w przepisach o ochronie danych osobowych.".

Art. 118. W ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2017 r. poz. 201, z późn. zm.[7)]) wprowadza się następujące zmiany:

1) w art. 14 § 4 otrzymuje brzmienie:

„§ 4. Minister właściwy do spraw finansów publicznych zapewnia funkcjonowanie portalu podatkowego i jest administratorem danych podatników, płatników, inkasentów, ich następców prawnych oraz osób trzecich korzystających z tego portalu.";

2) w art. 119zt pkt 4 otrzymuje brzmienie:

„4) Prezesa Urzędu Ochrony Danych Osobowych – w zakresie niezbędnym do realizacji ustawowych zadań określonych w przepisach o ochronie danych osobowych;";

3) w art. 119zzg wyrazy „Generalny Inspektor Ochrony Danych Osobowych" zastępuje się wyrazami „Prezes Urzędu Ochrony Danych Osobowych".

Art. 119. W ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876, z późn. zm.[8)]) w art. 105 w ust. 1 w pkt 2 lit. n otrzymuje brzmienie:

„n) Prezesa Urzędu Ochrony Danych Osobowych w zakresie niezbędnym do realizacji ustawowych zadań,".

Art. 120. W ustawie z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2018 r. poz. 110) w art. 6aa ust. 5 otrzymuje brzmienie:

„5. Agencja pełni funkcję administratora danych, o których mowa w ust. 2 i 3.".

---

7) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 648, 768, 935, 1428, 1537, 2169 i 2491 oraz z 2018 r. poz. 106,138 i 398.

8) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2361 i 2491 oraz z 2018 r. poz. 62, 106 i 138.

Art. 121. W ustawie z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów (Dz. U. poz. 763 i 1798 oraz z 2009 r. poz. 120 i 753) w art. 13 ust. 2 otrzymuje brzmienie:

„2. Jeżeli wyniki badań mają służyć nie tylko do informacji klienta, stosuje się przepisy o ochronie danych osobowych.”.

Art. 122. W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2018 r. poz. 23, 35, 106 i 138) wprowadza się następujące zmiany:

1) w art. 175a uchyla się § 2;
2) w art. 175c w § 1 uchyla się zdanie drugie.

Art. 123. W ustawie z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2017 r. poz. 1952 oraz z 2018 r. poz. 107 i 138) w art. 23 ust. 9 otrzymuje brzmienie:

„9. Informacje, o których mowa w ust. 8, mogą być przetwarzane przez ministra właściwego do spraw rodziny i wojewodę w celu monitorowania realizacji świadczeń rodzinnych oraz w celu umożliwienia organom właściwym i wojewodzie weryfikacji prawa do świadczeń rodzinnych oraz przez podmioty wymienione w ust. 10 w celu, w którym informacje te zostały im udostępnione, na zasadach określonych w przepisach o ochronie danych osobowych. Organy właściwe i wojewoda przekazują dane do rejestru centralnego, wykorzystując oprogramowanie, o którym mowa w ust. 7.”.

Art. 124. W ustawie z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (Dz. U. z 2018 r. poz. 56, z 2017 r. poz. 2491 oraz z 2018 r. poz. 106 i 138) w art. 286b ust. 16 otrzymuje brzmienie:

„16. Komisja może przekazać organowi nadzoru państwa trzeciego informacje dotyczące sprawy indywidualnej prowadzonej przez Komisję, jeżeli spełnione są warunki, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1) – w przypadku danych osobowych, oraz jeżeli ich przekazanie jest niezbędne dla realizacji zadań określonych ustawą. Komisja może w takim przypadku wyrazić zgodę na dalsze przekazanie tych informacji organowi nadzoru innego państwa trzeciego.”.

Art. 125. W ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2017 r. poz. 2168, 2290 i 2486 oraz z 2018 r. poz. 107 i 398) w art. 83 w ust. 2 w pkt 10 kropkę zastępuje się średnikiem i dodaje się pkt 11 w brzmieniu:

„11) kontroli przeprowadzanej w celu uzupełnienia dowodów w postępowaniu o stwierdzenie naruszenia danych osobowych.".

Art. 126. W ustawie z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz. U. z 2017 r. poz. 1311 i 2110) użyte w art. 47 w ust. 1 w pkt 11 i w art. 52 w pkt 8, w różnym przypadku, wyrazy „Generalny Inspektor Ochrony Danych Osobowych" zastępuje się użytymi w odpowiednim przypadku wyrazami „Prezes Urzędu Ochrony Danych Osobowych".

Art. 127. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570) wprowadza się następujące zmiany:

1) w art. 2 w ust. 4 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych" zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych";
2) w art. 4 pkt 1 otrzymuje brzmienie:

„1) przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1) i ustawy z dnia ... o ochronie danych osobowych (Dz. U. ...);".

Art. 128. W ustawie z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym (Dz. U. z 2017 r. poz. 2183 i 2201 oraz z 2018 r. poz. 138 i 398) w art. 88 uchyla się ust. 5.

Art. 129. W ustawie z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów (Dz. U. z 2017 r. poz. 2186 oraz z 2018 r. poz. 538) w art. 22 w ust. 1 w pkt 8c wyrazy „Generalnego Inspektora Ochrony Danych Osobowych" zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych".

Art. 130. W ustawie z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2018 r. poz. 554) w art. 15 ust. 8b otrzymuje brzmienie:

„8b. Informacje zawarte w rejestrze centralnym, o którym mowa w ust. 8a, mogą być przetwarzane przez ministra właściwego do spraw rodziny i wojewodę w celu monitorowania realizacji świadczeń z funduszu alimentacyjnego oraz w celu umożliwienia organom właściwym dłużnika i organom właściwym wierzyciela weryfikacji prawa do świadczeń z funduszu alimentacyjnego oraz przez podmioty wymienione w ust. 8c w celu, w którym informacje te zostały im udostępnione, na zasadach określonych w przepisach o ochronie danych osobowych. Organy właściwe wierzyciela oraz organy właściwe dłużnika przekazują dane do rejestru centralnego, wykorzystując oprogramowanie, o którym mowa w ust. 8.".

Art. 131. W ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62) w art. 139 w ust. 2 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych" zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych".

Art. 132. W ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, 2486 i 2491 oraz z 2018 r. poz. 62, 106 i 138) w art. 9f w ust. 1 pkt 18 otrzymuje brzmienie:

„18) na żądanie Prezesa Urzędu Ochrony Danych Osobowych, w zakresie wykonywania przez niego zadań określonych w przepisach o ochronie danych osobowych;".

Art. 133. W ustawie z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz. U. z 2018 r. poz. 470) w art. 11 w ust. 2 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych" zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych".

Art. 134. W ustawie z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. z 2017 r. poz. 631 i 1321 oraz z 2018 r. poz. 138) w art. 18 w ust. 2 w pkt 6 wyrazy „Generalny Inspektor Ochrony Danych Osobowych" zastępuje się wyrazami „Prezes Urzędu Ochrony Danych Osobowych".

Art. 135. W ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412) w art. 34 w ust. 10 w pkt 9 wyrazy „Generalnego Inspektora Ochrony

Danych Osobowych" zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych".

Art. 136. W ustawie z dnia 5 stycznia 2011 r. – Kodeks wyborczy (Dz. U. z 2017 r. poz. 15 i 1089 oraz z 2018 r. poz. 4, 130 i 138) w art. 143 § 4 otrzymuje brzmienie:

„§ 4. Wykaz wpłat obywateli polskich na rzecz komitetu wyborczego organizacji i komitetu wyborczego wyborców Państwowa Komisja Wyborcza i komisarz wyborczy udostępniają do wglądu na wniosek, w trybie i na zasadach określonych w przepisach o ochronie danych osobowych.".

Art. 137. W ustawie z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2018 r. poz. 123) w art. 27 ust. 9 otrzymuje brzmienie:

„9. Postępowanie w sprawach określonych w ust. 1–6 jest poufne i odbywa się z zachowaniem przepisów o ochronie danych osobowych.".

Art. 138. W ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2017 r. poz. 2003 oraz z 2018 r. poz. 62) art. 10 otrzymuje brzmienie:

„Art. 10. Dostawcy i podmioty prowadzące systemy płatności mogą przetwarzać dane osobowe w zakresie niezbędnym do zapobiegania oszustwom związanym z wykonywanymi usługami płatniczymi lub prowadzeniem systemu płatności oraz dochodzenia i wykrywania tego rodzaju oszustw przez właściwe organy, z wyjątkiem danych, o których mowa w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).".

Art. 139. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2018 r. poz. 21 oraz z 2017 r. poz. 2422) w art. 80 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) zapewnia bezpieczeństwo przetwarzanych danych, informacji oraz dokumentów, które otrzymał w związku z prowadzeniem BDO, zgodnie z przepisami o ochronie danych osobowych.".

Art. 140. W ustawie z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (Dz. U. z 2017 r. poz. 1148, 1213 i 1593 oraz z 2018 r. poz. 9) w art. 159 ust. 1 otrzymuje brzmienie:

„1. Prezes UDT administruje i przetwarza dane zawarte w rejestrach, o których mowa w art. 158 ust. 1, zgodnie z przepisami o ochronie danych osobowych.".

Art. 141. W ustawie z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach (Dz. U. z 2018 r. poz. 408) w art. 15 ust. 3 otrzymuje brzmienie:

„3. Decyzję o zakazie zgromadzenia udostępnia się w Biuletynie Informacji Publicznej z uwzględnieniem przepisów o ochronie danych osobowych przez 3 miesiące od dnia jej wydania.".

Art. 142. W ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2017 r. poz. 1170, z późn. zm.[9)]) w art. 35 w ust. 2 pkt 10 otrzymuje brzmienie:

„10) Prezesa Urzędu Ochrony Danych Osobowych, w zakresie wykonywania przez niego zadań określonych w przepisach o ochronie danych osobowych;".

Art. 143. W ustawie z dnia 25 września 2015 r. o zawodzie fizjoterapeuty (Dz. U. z 2018 r. poz. 505) w art. 12 ust. 9 otrzymuje brzmienie:

„9. Postępowanie w sprawach określonych w ust. 1–7 jest poufne i odbywa się z zachowaniem przepisów o ochronie danych osobowych.".

Art. 144. W ustawie z dnia 9 października 2015 r. o produktach biobójczych (Dz. U. z 2018 r. poz. 122 i 138) w art. 42 ust. 2 otrzymuje brzmienie:

„2. Raport oraz dane, o których mowa w ust. 1, nie mogą obejmować danych podlegających ochronie na podstawie przepisów o ochronie danych osobowych.".

Art. 145. W ustawie z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5) wprowadza się następujące zmiany:

1) w art. 13 § 5 otrzymuje brzmienie:

„§ 5. Prokurator Generalny jest administratorem danych przetwarzanych w ogólnokrajowych systemach teleinformatycznych jednostek organizacyjnych prokuratury.";

2) w art. 191 uchyla się § 2.

Art. 146. W ustawie z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz. U. z 2017 r. poz. 1851 oraz z 2018 r. poz. 107 i 138) w art. 14 ust. 3 otrzymuje brzmienie:

[9)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 1089, 1926, 2102 i 2486 oraz z 2018 r. poz. 8 i 106.

„3. Informacje, o których mowa w ust. 2, mogą być przetwarzane przez ministra właściwego do spraw rodziny i wojewodę w celu monitorowania realizacji świadczeń wychowawczych oraz w celu umożliwienia organom właściwym i wojewodom weryfikacji prawa do świadczeń wychowawczych oraz przez podmioty wymienione w ust. 4 w celu, w jakim informacje te zostały im udostępnione, na zasadach określonych w przepisach o ochronie danych osobowych. Organy właściwe i wojewodowie przekazują dane do rejestru centralnego, wykorzystując systemy teleinformatyczne, o których mowa w ust. 1.".

Art. 147. W ustawie z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 352 oraz z 2017 r. poz. 60) w art. 7 ust. 2 otrzymuje brzmienie:

„2. Przepisy ustawy nie naruszają przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1) i ustawy z dnia ... o ochronie danych osobowych (Dz. U. ...).".

Art. 148. W ustawie z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (Dz. U. z 2018 r. poz. 410) art. 9 otrzymuje brzmienie:

„Art. 9. Do danych osobowych zgromadzonych w systemie zgłaszania stosuje się przepisy o ochronie danych osobowych.".

Art. 149. W ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2018 r. poz. 508) w art. 45 ust. 1 otrzymuje brzmienie:

„1. Organy KAS, w celu realizacji ustawowych zadań w zakresie, o którym mowa w art. 2 ust. 1 pkt 1, 2, 6 i 8, mogą zbierać i wykorzystywać informacje, w tym dane osobowe, od osób prawnych, jednostek organizacyjnych niemających osobowości prawnej oraz osób fizycznych prowadzących działalność gospodarczą, o zdarzeniach mających bezpośredni wpływ na powstanie lub wysokość zobowiązania podatkowego lub należności celnych, oraz przetwarzać, a także występować do tych podmiotów o udostępnienie dokumentów zawierających informacje, w tym dane osobowe, także bez wiedzy i zgody osoby, której dane te dotyczą.".

Art. 150. W ustawie z dnia 9 marca 2017 r. o systemie monitorowania drogowego przewozu towarów (Dz. U. poz. 708 oraz z 2018 r. poz. 138) w art. 4 ust. 3 otrzymuje brzmienie:

„3. Rejestr prowadzi Szef Krajowej Administracji Skarbowej, który jest administratorem danych przetwarzanych w rejestrze.".

Art. 151. W ustawie z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz. U. poz. 2217) w art. 10 ust. 5 otrzymuje brzmienie:

„5. Wypełnione deklaracje wyboru, o których mowa w ust. 1 pkt 1, świadczeniodawca przechowuje w swojej siedzibie albo w miejscu udzielania świadczeń z zakresu podstawowej opieki zdrowotnej, zapewniając ich dostępność świadczeniobiorcom, którzy je złożyli, z zachowaniem wymagań wynikających z przepisów o ochronie danych osobowych.".

Rozdział 13

Przepisy przejściowe i dostosowujące

Art. 152. 1. Osoba pełniąca w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, o którym mowa w ustawie uchylanej w art. 168, staje się inspektorem ochrony danych i pełni swoją funkcję do dnia 1 września 2018 r., chyba że przed tym dniem administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na inspektora ochrony danych, w sposób określony w art. 10 ust. 1.

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

3. Osoba, o której mowa w ust. 1, może zostać odwołana przez administratora bez zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na inspektora ochrony danych, w przypadku gdy na podstawie art. 37 rozporządzenia 2016/679 administrator nie jest obowiązany do wyznaczenia inspektora ochrony danych.

4. Administrator, który do dnia wejścia w życie ustawy nie powołał administratora bezpieczeństwa informacji, o którym mowa w ustawie uchylanej w art. 168, jest obowiązany do wyznaczenia inspektora ochrony danych na podstawie art. 37 rozporządzenia 2016/679 i zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu, w terminie do dnia 31 lipca 2018 r.

5. Podmiot przetwarzający, obowiązany do wyznaczenia inspektora ochrony danych na podstawie art. 37 rozporządzenia 2016/679, wyznacza inspektora ochrony danych i zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu, w sposób określony w art. 10 ust. 1, w terminie do dnia 31 lipca 2018 r.

Art. 153. 1. Do kontroli wszczętej i niezakończonej przed dniem wejścia w życie ustawy stosuje się przepisy dotychczasowe.

2. Upoważnienia oraz legitymacje służbowe wydane przed dniem wejścia w życie ustawy zachowują ważność do czasu zakończenia kontroli, o której mowa w ust. 1.

Art. 154. 1. Postępowania prowadzone przed Generalnym Inspektorem Ochrony Danych Osobowych, wszczęte i niezakończone przed dniem wejścia w życie ustawy, prowadzone są przed Prezesem Urzędu Ochrony Danych Osobowych.

2. Postępowania, o których mowa w ust. 1, prowadzi się na podstawie przepisów ustawy uchylanej w art. 168, zgodnie z zasadami określonymi w przepisach ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Czynności dokonane w postępowaniach, o których mowa w ust. 1, pozostają skuteczne.

4. Postępowania prowadzone na podstawie rozdziału 6 ustawy uchylanej w art. 168 umarza się. Decyzji o umorzeniu postępowania nie wydaje się.

Art. 155. Podmiot, do którego przed dniem wejścia w życie ustawy zostało skierowane wystąpienie lub wniosek, o którym mowa w art. 19a ustawy uchylanej w art. 168, jest obowiązany przekazać Prezesowi Urzędu Ochrony Danych Osobowych odpowiedź na wystąpienie lub wniosek w terminie 30 dni od dnia wejścia w życie ustawy.

Art. 156. 1. W przypadku postępowań egzekucyjnych prowadzonych na podstawie tytułu wykonawczego wystawionego przez Generalnego Inspektora Ochrony Danych Osobowych przed dniem wejścia w życie ustawy i niezakończonych do dnia jej wejścia w życie, wierzycielem staje się Prezes Urzędu Ochrony Danych Osobowych.

2. Czynności dokonane przez Generalnego Inspektora Ochrony Danych Osobowych w postępowaniu, o którym mowa w ust. 1, pozostają skuteczne.

Art. 157. Podjęte w postępowaniach egzekucyjnych wszczętych na podstawie przepisów ustawy zmienianej w art. 110 i niezakończonych przed dniem wejścia w życie ustawy, wysłane upomnienia, tytuły wykonawcze, postanowienia zawierające stanowisko

Generalnego Inspektora Ochrony Danych Osobowych oraz inne czynności dokonane przez Generalnego Inspektora Ochrony Danych Osobowych, jako wierzyciela, pozostają skuteczne.

Art. 158. Postępowania w sprawie stanowiska Generalnego Inspektora Ochrony Danych Osobowych, jako wierzyciela, wszczęte na podstawie art. 34 ustawy zmienianej w art. 110 i niezakończone przed dniem wejścia w życie ustawy są prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych.

Art. 159. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 22a ustawy uchylanej w art. 168, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 48 niniejszej ustawy, nie dłużej niż 12 miesięcy od dnia jej wejścia w życie.

Art. 160. 1. Z dniem wejścia w życie ustawy Generalny Inspektor Ochrony Danych Osobowych staje się Prezesem Urzędu Ochrony Danych Osobowych.

2. Osoba, która została powołana na stanowisko Generalnego Inspektora Ochrony Danych Osobowych, na podstawie ustawy uchylanej w art. 168, pozostaje na stanowisku do czasu upływu kadencji, na którą została powołana.

3. Zastępca Generalnego Inspektora Ochrony Danych Osobowych, powołany przed dniem wejścia w życie ustawy staje się z dniem wejścia w życie ustawy zastępcą Prezesa Urzędu, o którym mowa w art. 36 ust. 1.

Art. 161. 1. Z dniem wejścia w życie ustawy Biuro Generalnego Inspektora Ochrony Danych Osobowych staje się Urzędem Ochrony Danych Osobowych.

2. Z dniem wejścia w życie ustawy pracownicy zatrudnieni w Biurze Generalnego Inspektora Ochrony Danych Osobowych stają się pracownikami Urzędu Ochrony Danych Osobowych. Przepis art. 23^1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy stosuje się odpowiednio.

Art. 162. Z dniem wejścia w życie ustawy mienie Skarbu Państwa będące we władaniu Biura Generalnego Inspektora Ochrony Danych Osobowych staje się mieniem będącym we władaniu Urzędu Ochrony Danych Osobowych.

Art. 163. Należności i zobowiązania Biura Generalnego Inspektora Ochrony Danych Osobowych z dniem wejścia w życie ustawy stają się należnościami i zobowiązaniami Urzędu Ochrony Danych Osobowych.

Art. 164. W przypadku gdy Generalny Inspektor Ochrony Danych Osobowych do dnia wejścia w życie ustawy nie złoży sprawozdania ze swojej działalności, sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych składa Prezes Urzędu Ochrony Danych Osobowych w terminie do dnia 31 lipca 2018 r.

Art. 165. 1. W sprawach sądowych, sądowoadministracyjnych lub administracyjnych, w których stroną lub uczestnikiem był Generalny Inspektor Ochrony Danych Osobowych, z dniem wejścia w życie ustawy stroną lub uczestnikiem staje się Prezes Urzędu Ochrony Danych Osobowych.

2. W sprawach sądowych, sądowoadministracyjnych lub administracyjnych, w których stroną lub uczestnikiem było Biuro Generalnego Inspektora Ochrony Danych Osobowych, z dniem wejścia w życie ustawy stroną lub uczestnikiem staje się Urząd Ochrony Danych Osobowych.

Art. 166. Prezes Urzędu wyda pierwszy komunikat, o którym mowa w art. 55 ust. 1 pkt 1, w terminie 3 miesięcy od dnia wejścia w życie ustawy.

Rozdział 14

Przepisy końcowe

Art. 167. 1. Maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy wynosi w roku:

1) 2018 – 19 639 000 zł;
2) 2019 – 13 541 000 zł;
3) 2020 – 13 860 000 zł;
4) 2021 – 13 860 000 zł;
5) 2022 – 13 860 000 zł;
6) 2023 – 13 860 000 zł;
7) 2024 – 13 860 000 zł;
8) 2025 – 13 860 000 zł;
9) 2026 – 13 860 000 zł;
10) 2027 – 13 860 000 zł.

2. Prezes Urzędu Ochrony Danych Osobowych monitoruje wykorzystanie limitu wydatków, o których mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału.

3. W przypadku przekroczenia lub zagrożenia przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków określonego w ust. 1 oraz w przypadku, gdy w okresie od początku roku kalendarzowego do dnia ostatniej oceny, o której mowa w ust. 2, część limitu rocznego przypadającego proporcjonalnie na ten okres zostanie przekroczona co najmniej o 10%, stosuje się mechanizm korygujący polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym ustawy.

4. Organem właściwym do wdrożenia mechanizmu korygującego, o którym mowa w ust. 3, jest Prezes Urzędu Ochrony Danych Osobowych.

Art. 168. Traci moc ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138).

Art. 169. Ustawa wchodzi w życie z dniem 25 maja 2018 r.

UZASADNIENIE

Opracowanie projektu nowej ustawy o ochronie danych osobowych wynika z konieczności zapewnienia stosowania 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".

Rozporządzenie będzie obowiązywało w polskim porządku prawnym bezpośrednio i będzie miało zastosowanie od dnia 25 maja 2018 r., i od tego dnia polskie przepisy muszą zapewniać skuteczne stosowanie przepisów Rozporządzenia, nie powielając jego rozwiązań ani nie będąc z nim sprzecznymi. Zakres kompetencji państw członkowskich wdrażania przepisów Rozporządzenia wyznacza co do zasady samo rozporządzenie (zob. szerzej P. Kozik, „Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego" EPS 5/2017 s. 18-22).

Przepisy obowiązującej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), zwanej dalej „obowiązującą Ustawą", z jednej strony zawierają regulacje analogiczne do regulacji Rozporządzenia, np. w zakresie definicji danych osobowych, z drugiej zawierają regulacje odmienne niż te, które przewiduje Rozporządzenie, choćby w zakresie definicji zgody osoby, której dane dotyczą. Obowiązująca Ustawa zawiera też regulacje, których nie przewiduje Rozporządzenie, np. w zakresie rejestracji zbiorów danych, ale także brak w obowiązującej ustawie przepisów dotyczących choćby certyfikacji.

W świetle powyższego konieczne stało się opracowanie zupełnie nowej regulacji w zakresie ochrony danych osobowych, która odpowiadałaby przepisom i standardom ochrony danych osobowych przyjętym na poziomie UE. Przepisy projektowanej ustawy ustanawiają nowy organ właściwy w sprawie ochrony danych osobowych – będzie nim Prezes Urzędu Ochrony Danych Osobowych.

Rozdział 1 Przepisy ogólne

W Rozdziale 1 wskazano zakres regulacji. Zgodnie z art. 1, ustawa będzie miała zastosowanie do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych.

Państwa członkowskie nie mają kompetencji prawodawczej do określenia relacji pomiędzy Rozporządzeniem a przepisami implementującymi inne akty prawa wtórnego UE, w tym dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW. Projekt jest aktem prawnym zapewniającym skuteczne stosowanie przepisów Rozporządzenia, nie implementuje jednak przepisów wskazanej dyrektywy, odnosząc się do niej w swojej treści wyłącznie w niewielkim stopniu.

Wobec powyższego przepisy ustawy nie znajdą zastosowania do ochrony innych podmiotów w związku z przetwarzaniem ich danych osobowych. Powyższe odpowiada zakresowi podmiotowemu zastosowania Rozporządzenia i jest zgodne z motywem 14 preambuły do Rozporządzenia, który stanowi, że: „Ochrona zapewniana niniejszym Rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych. Niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych, dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej.". W ocenie projektodawcy, pojęcie „osoby prawnej" powinno być intepretowane w świetle legislacji krajowej, obejmując również swoim zakresem tzw. ułomne osoby prawne. Pojęcie danych o firmie i formie prawnej oraz danych kontaktowych powinno obejmować dane konieczne do oznaczania osoby prawnej w obrocie gospodarczym, przy czym nie jest możliwym uznanie, że są to wszystkie dane zawarte przykładowo w Krajowym Rejestrze Sądowym. W ocenie projektodawcy nie powinny być to dane, które przykładowo wskazują na rozdzielność majątkową członka zarządu spółki. Jednocześnie nie zdecydowano się skorzystać z możliwości przyjęcia przepisów o przetwarzaniu danych osobowych osób zmarłych. W tym zakresie instrumentem ochrony będą przepisy o ochronie dóbr osobistych przewidziane w ustawie z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2017 r. poz. 459, 933, 1132 oraz z 2018 r. poz. 398 i 650) (np. w ramach kultu pamięci osoby zmarłej).

W projekcie ustawy przyjęto, że przedmiotowy zakres jej zastosowania będzie odpowiadał zakresowi zastosowania Rozporządzenia, co oznacza, że będzie miała zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz

do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących lub mających stanowić część zbioru danych. Poza organami i instytucjami powoływanymi na podstawie Rozporządzenia, adresatami wynikających z niego obowiązków są z kolei administratorzy, podmioty przetwarzające.

Stosowanie nowej ustawy – zgodnie z treścią Rozporządzenia – będzie wyłączone w odniesieniu do przetwarzania danych osobowych:

1) w ramach działalności nieobjętej zakresem prawa Unii;

2) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 Traktatu o funkcjonowaniu Unii Europejskiej;

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

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

Projektodawca przyjął w projekcie nowej ustawy dokładnie taki sam zakres przedmiotowy, jak w przypadku Rozporządzenia, uznając, iż jest on adekwatnie szeroki, podobnie jak w obowiązującej Ustawie. Jednocześnie przyjął, że wyjątki od stosowania nowej ustawy stanowią katalog zamknięty i muszą być stosowane zawężająco. Stąd w trakcie prac nad projektem nowej ustawy rozważano, jakie sprawy będą mogły być wyłączone z zakresu jej stosowania jako działalność nieobjęta prawem UE. Ostatecznie przyjęto, że wyłączenie to ma bardzo wąski charakter, gdyż działania podejmowane przez państwa członkowskie, w których mamy do czynienia z przetwarzaniem danych osobowych, będą podlegały regułom wynikającym z Rozporządzenia, ze względu na konieczność zapewnienia tym danym ochrony na takich samych warunkach we wszystkich państwach członkowskich. Projektodawca nie zdecydował się również na poszerzenie zakresu zastosowania Rozporządzenia na obszary objęte kompetencjami koordynacyjnymi, przewidzianymi w art. 6 Traktatu o funkcjonowaniu Unii Europejskiej. Wejście w życie Traktatu z Lizbony wprowadziło bowiem w tym zakresie znaczącą zmianę. Traktat zniósł strukturę filarową w UE oraz wprowadził ogólną podstawę prawną do przyjęcia jednolitych ram prawnych ochrony danych osobowych w art. 16 TFUE,

obejmując nimi były I oraz III filar UE. Obszary te objęte są więc działalnością unifikacyjną Unii Europejskiej w zakresie objętym Rozporządzeniem.

Jednocześnie, biorąc pod uwagę potrzebę jednolitego stosowania Rozporządzenia, nie zdecydowano się na poziomie projektowanej ustawy zdefiniować pojęć wyznaczających zakres wyłączeń stosowania Rozporządzenia. Projektodawca – mimo podobnych działań podejmowanych przez inne państwa członkowskie, nie zdecydował się również na ograniczenie zastosowania przepisów o ochronie danych osobowych wyłącznie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Polsce, uznając, że stanowiłoby to ograniczenie art. 3 Rozporządzenia. Szczegółowy zakres przedmiotowy projektowanej ustawy określa art. 1 ust. 2 projektu.

Projektodawca zdecydował się wprowadzić do projektu przepis, określający zakres zastosowania przepisów o ochronie danych osobowych dla bezpieczeństwa narodowego państwa. W polskiej legislacji brak jest zamkniętego katalogu działań, uznanych za wchodzące w zakres „bezpieczeństwa narodowego". W ocenie projektodawcy decyzja o tym, czy dane działanie uznane powinno być za objęte „bezpieczeństwem narodowym", podjęta powinna być po wnikliwej ocenie każdego stanu faktycznego przez administratora oraz podmiot przetwarzający. Przy czym nie powinno się stosować w tym przypadku wykładni zawężającej ochronę prawa podstawowego, jakim jest ochrona danych osobowych. Decyzja taka będzie w dalszej kolejności podlegała działaniom kontrolnym Prezesa Urzędu oraz wymiaru sprawiedliwości. Projektodawca nie zdecydował się przesądzić relacji zachodzących pomiędzy art. 2 ust. 2 lit. a Rozporządzenia oraz art. 23 ust. 1 lit. a Rozporządzenia w kontekście możliwego użycia w nich tej samej klauzuli „bezpieczeństwa narodowego". TSUE w wyroku Bodil Lindqvist C 101/01 (Wyrok TSUE z 6.11.2003 w sprawie C-101/01, Lindqvist, EU:C:2003:596) wskazał, że: „rodzaje działalności wymienione tytułem przykładu w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 (a mianowicie rodzaje działalności, o których stanowią tytuły V i VI Traktatu o Unii Europejskiej, jak również przetwarzanie w ramach działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa oraz w ramach działalności państwa w obszarach prawa karnego) stanowią w każdym razie działania właściwe państwom i władzom państwowym, obce dziedzinom działalności jednostek.". W ocenie projektodawcy odmiennie będzie traktowana sytuacja w obrębie art. 23 Rozporządzenia, ponieważ w tym wypadku bezpieczeństwo narodowe jest jedynie środkiem służącym temu bezpieczeństwu, a nie celem samym w sobie. Innymi słowy istota

działalności podmiotu, który będzie korzystał z ograniczenia z art. 23 Rozporządzenia, nie będzie ukierunkowana bezpośrednio na bezpieczeństwo narodowe, lecz na inne obszary działalności podlegające prawodawstwu unijnemu. Zakresy art. 2 ust. 2 lit. a , w zw. z art. 4 ust. 2 TUE i art. 23 ust. 1 Rozporządzenia nie pokrywają się, pomimo użycia tej samej klauzuli „bezpieczeństwa narodowego".

Uwzględniając, że ustawa służy zapewnieniu skutecznego stosowania w polskiej przestrzeni prawnej Rozporządzenia, jego treść wyznacza zakres terytorialny jej stosowania. Tym samym ustawę stosuje się do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

Nowa ustawa – zgodnie z przepisami Rozporządzenia – będzie miała zastosowanie także do przetwarzania danych osób przebywających w Unii, przez administratora lub podmiot przetwarzający niemający jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty, lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

Nowa ustawa będzie też stosowana do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

W przepisach ogólnych projektowanej ustawy, w art. 2, wyłączono stosowanie niektórych przepisów Rozporządzenia do:

– działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych,

– wypowiedzi w ramach działalności literackiej,

– wypowiedzi w ramach działalności artystycznej,

– wypowiedzi akademickiej.

W przypadku wszystkich ww. rodzajów wypowiedzi akademickiej wyłączono stosowanie art. 13, art. 15 ust. 3 i 4, art. 18, art. 27, art. 28 ust. 2-10 oraz art. 30 Rozporządzenia.

Wyłączono zatem następujące obowiązki administratora lub podmiotu przetwarzającego:

– informowanie osoby, której dane dotyczą, o danych pozyskanych od tej osoby (art. 13),

– dostarczanie osobie, której dane dotyczą, kopii danych (art. 15 ust. 3 oraz ust. 4),

– ograniczenie przetwarzania na wniosek osoby, której dane dotyczą (art. 18),

– wyznaczanie swojego przedstawiciela w UE w przypadku, o którym mowa w art. 3 ust. 2 Rozporządzenia (art. 27),

– powierzenie przetwarzania danych osobowych podmiotowi przetwarzającemu na podstawie umowy lub innego instrumentu prawnego (art. 28),

– prowadzenie rejestru czynności przetwarzania danych osobowych (art. 30).

Dodatkowo do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych, działalności literackiej oraz działalności artystycznej nie będzie się stosowało następujących przepisów Rozporządzenia:

– art. 5 – zasady przetwarzania danych osobowych,

– art. 6 – przesłanki legalności przetwarzania danych osobowych,

– art. 7 – warunki wyrażania zgody przez osobę, której dane dotyczą,

– art. 8 – warunki wyrażania zgody przez dziecko w przypadku usług społeczeństwa informacyjnego,

– art. 9 – przetwarzanie szczególnych kategorii danych,

– art. 11 – przetwarzanie danych osobowych osoby niewymagającej identyfikacji,

– art. 14 – obowiązek podawania informacji w przypadku pozyskiwania danych nie od osoby, której dane dotyczą,

– art. 15 ust. 1 i 2 – prawo dostępu przysługujące osobie, której dane dotyczą,

– art. 16 – prawo do sprostowania danych,

– art. 19 – obowiązek powiadomienia odbiorcy danych o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,

– art. 20 – prawo do przenoszenia danych,

– art. 21 – prawo do sprzeciwu,

– art. 22 – zautomatyzowane podejmowanie decyzji w indywidualnych sprawach, w tym profilowanie.

W ocenie projektodawcy ww. wyłączenia „realizują" motyw 153 Rozporządzenia, zgodnie z którym: „Prawo państw członkowskich powinno godzić przepisy, regulujące wolność wypowiedzi i informacji, w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia. Przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, przewidzianymi w art. 11 Karty praw podstawowych. Powinno mieć to zastosowanie w szczególności do przetwarzania danych osobowych w dziedzinie audiowizualnej oraz w archiwach i bibliotekach prasowych. Państwa członkowskie powinny więc przyjąć akty prawne określające odstępstwa i wyjątki niezbędne do zapewnienia równowagi między tymi prawami podstawowymi. Państwa członkowskie powinny przyjąć takie odstępstwa i wyjątki w odniesieniu do zasad ogólnych, praw przysługujących osobie, której dane dotyczą, administratora i podmiotu przetwarzającego, przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, niezależnych organów nadzorczych, współpracy i spójności oraz szczególnych sytuacji przetwarzania danych. Jeżeli odstępstwa i wyjątki różnią się zależnie od państwa członkowskiego, zastosowanie powinno mieć prawo państwa członkowskiego, któremu podlega administrator. Aby uwzględnić, jak ważna dla każdego demokratycznego społeczeństwa jest wolność wypowiedzi, pojęcia dotyczące tej wolności, takie jak dziennikarstwo, należy interpretować szeroko.". Art. 85 Rozporządzenia przewiduje możliwość ograniczenia przepisów odnoszących się do ochrony danych osobowych, jedynie gdy jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji. Ocena taka podjęta została na etapie tworzenia projektu.

W pierwszej kolejności należy wskazać, że ustawodawca unijny w przepisach rozporządzenia 2016/679 wprowadza dwa rodzaje testów, których przeprowadzenie warunkuje możliwość skorzystania przez państwa członkowskie z ograniczeń w stosowaniu rozporządzenia 2016/679 w określonych celach. Pierwszym z nich jest przewidziany w art. 23 rozporządzenia 2016/679 test „niezbędności i proporcjonalności", a drugim jest przewidziany chociażby w art. 85 rozporządzenia test „niezbędności". O ile, jak zostało to wskazane w art. 23 rozporządzenia i odnoszącym się do niego motywie 73 preambuły do rozporządzenia 2016/679 „w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz praw (...) o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym", wymogu proporcjonalności nie przewiduje już ustawodawca unijny w art. 85 rozporządzenia. Zgodnie z odnoszącym się do art. 85 motywem 153 preambuły do rozporządzenia 2016/679 „przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji". Powołanie się na art. 85 rozporządzenia 2016/679 i skorzystanie z przewidzianej w nim swobody regulacyjnej państwa członkowskiego nie wymaga dokonania więc oceny proporcjonalności proponowanych ograniczeń, a jedynie ich niezbędność. Dodatkowo należy wskazać, że ustawodawca unijny w art. 85 nie wskazuje konkretnych przepisów podlegających możliwemu ograniczeniu, jak zrobił to w art. 23, wskazując jedynie rozdziały. Tym samym ustawodawca unijny przyznał w art. 85 bardzo szeroki zakres swobody regulacyjnej państwom członkowskim, dostrzegając szczególną wartość działań dziennikarskich oraz artystycznych i akademickich. Dokonując wykładni testu niezbędności, Trybunał Konstytucyjny w wyroku z 5 lutego 2008 r. sygn. akt. K 34/06 wskazał, że nakłada on na ustawodawcę „wymóg stwierdzenia rzeczywistej potrzeby dokonania w danym stanie faktycznym ingerencji w zakres prawa bądź wolności jednostki. Z drugiej zaś, winna ona być rozumiana jako wymóg stosowania takich środków prawnych, które będą skuteczne, a więc rzeczywiście służące realizacji zamierzonych przez prawodawcę celów. Ponadto chodzi tu o środki niezbędne, w tym sensie, że chronić będą określone wartości w sposób bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków. Niezbędność to również skorzystanie ze środków jak najmniej uciążliwych dla podmiotów, których prawa lub wolności ulegną ograniczeniu". W ocenie projektodawcy każde z projektowanych ograniczeń w obszarze działalności literackiej, działalności artystycznej, wypowiedzi akademickiej oraz działaniach związanych z tworzeniem

materiałów prasowych spełnia powyższe wymogi. W szczególności brak wyłączenia przewidzianego w art. 13 rozporządzenia 2016/679 obowiązku informowania osoby, której dane dotyczą, o danych pozyskanych od tej osoby w ramach wypowiedzi akademickiej wyłączyłby w zasadzie możliwość prowadzenia działań dydaktycznych na uczelniach wyższych, wykładach otwartych dla wolnych słuchaczy itd. Prowadzący takie zajęcia nie mógłby dla celów związanych z prowadzonym wykładem zebrać danych uczestników wykładu, bez konieczności zrealizowania wobec nich długiego obowiązku, co często przekroczyłoby czas przeznaczony na sam wykład. Jednocześnie forma wypowiedzi akademickiej sama w sobie przesądza, że osoby takie znają cel i dane osoby pozyskującej dane. Z kolei brak wyłączenia prawa do wystąpienia z żądaniem ograniczenia przetwarzania na wniosek osoby, której dane dotyczą, mogłoby w ocenie projektodawcy skutkować niemożnością opublikowania wyników badań naukowych. Wypowiedzią akademicką jest bowiem również działalność polegająca na publikowaniu materiałów naukowych na uczelni wyższej. Zrealizowanie skuteczne prawa do ograniczenia danych prowadziłoby do zniekształcenia źródeł będących podstawą stawianych w ramach wypowiedzi akademickiej tez badawczych.

W przypadku działalności polegającej na tworzeniu materiałów prasowych oraz działalności artystycznej i literackiej wyłączono w szczególności zastosowanie prawa dostępu do danych osobowych. W ocenie projektodawcy w wielu przypadkach uzyskanie takiego prawa mogłoby wiązać się z ujawnieniem tajemnicy dziennikarskiej, wpływając również na proces tworzenia materiałów prasowych oraz proces twórczy. Ciężko sobie bowiem wyobrazić sytuację, w której twórca spektaklu lub dziennikarz miałby pracować pod presją tego, że przed opublikowaniem materiału prasowego lub premierą sztuki ktoś udostępni opracowywane przez nich treści, uzyskując dostęp do danych. Ograniczono również zastosowanie obowiązku podawania informacji w przypadku pozyskiwania danych nie od osoby, której dane dotyczą, co w ocenie projektodawcy mogłoby wpłynąć chociażby na ograniczenie tajemnicy dziennikarskiej. Obowiązek przekazania informacji o źródle pozyskanych danych mógłby w ogromnym stopniu wpłynąć na działanie polskiej prasy, wpływając również na subiektywizm publikowanych treści. Projektodawca proponuje również wyłączenie prawa do sprostowania danych, co mogłoby skutkować zafałszowaniem procesu twórczego, a w przypadku działalności dziennikarskiej szczególne uprawnienie w tym zakresie przysługuje na podstawie właściwych przepisów sektorowych.

Art. 85 Rozporządzenia nie zawiera wymogu wskazania w treści przepisów wprowadzających odstępstwa (od ogólnych wymogów), iż są one realizowane w celu pogodzenia prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji. Wprowadzenie takiego zastrzeżenia w praktyce w dużej mierze ograniczyłoby możliwość stosowania wyłączenia ze względu na praktyczne problemy z wykładnią niedookreślonych zwrotów: prawa do ochrony danych osobowych oraz wolności wypowiedzi i informacji. Zgodnie z treścią art. 85 Rozporządzenia państwa członkowskie na etapie legislacyjnym mogą wyważyć wskazane w tym przepisie wartości i na tej podstawie wyłączyć lub ograniczyć powołane tam obowiązki i prawa związane z ochroną danych osobowych.

Przepis zakłada skorzystanie przez polskiego ustawodawcę z możliwości ograniczenia stosowania części obowiązków informacyjnych, która została przewidziana w art. 23 Rozporządzenia. Na jego podstawie państwa członkowskie mogą wprowadzić wyłączenia w stosunku do ściśle wymienionych obowiązków i praw, jeśli nie spowoduje to naruszenia istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym jednemu z wymienionych celów. Rozporządzenie wskazuje, że ingerencja państwa członkowskiego musi służyć jednej z wymienionych przesłanek, m.in. bezpieczeństwu narodowemu, obronie, bezpieczeństwu publicznemu czy „innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego".

Zgodnie z Rozporządzeniem ograniczenie może dotyczyć takich praw i obowiązków, jak np. obowiązek podawania wskazanych informacji podczas zbierania danych osobowych od osoby, prawo dostępu do danych przysługujących osobie, której dane dotyczą, prawo do sprostowania danych, „prawo do bycia zapomnianym", prawo do ograniczenia przetwarzania czy prawa do przenoszenia danych.

Projekt wprowadza na podstawie art. 23 rozporządzenia 2016/679 ograniczenia stosowania:

1) art. 13 ust. 3 rozporządzenia 2016/679, który nakłada na administratora danych obowiązek informowania osoby, której dane dotyczą, o fakcie dalszego przetwarzania danych w innym celu niż cel, w którym dane osobowe zostały zebrane. Zgodnie z art. 13 ust. 3 rozporządzenia 2016/679 spełnienie obowiązku informacyjnego powinno nastąpić przed dalszym przetwarzaniem;

2) art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, zgodnie z którym w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, administrator danych musi spełnić wobec osoby, której dane dotyczą, szereg obowiązków informacyjnych, a także poinformować osobę, której dane dotyczą, o fakcie dalszego przetwarzania danych w innym celu niż cel, w którym dane osobowe zostały zebrane;

3) art. 15 ust. 1 – 3 rozporządzenia 2016/679 określającego prawo dostępu do informacji o fakcie przetwarzania danych przez administratora przysługujące osobie, której dane dotyczą. Przepisy te nie będą miały zastosowania, o ile osoba nie będzie informowana na podstawie art. 14 rozporządzenia 2016/679.

Z powyższego ograniczenia będą mogły skorzystać wyłącznie podmioty realizujące zadania publiczne. Możliwość skorzystania z tego ograniczenia uzależniona jest od spełnienia następujących warunków:

1) zmiana celu przetwarzania służy realizacji zadania publicznego;

2) niewykonanie obowiązku informacyjnego jest niezbędne dla realizacji celów określonych w art. 23 rozporządzenia 2016/679;

3) przekazanie informacji wymaganych przez art. 13 ust. 3 rozporządzenia 2016/679:

   a) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego, lub

   b) naruszy ochronę informacji niejawnych.

Jako przykład praktycznego zastosowania tych przepisów można wskazać sytuację, w której administrator na podstawie przepisów prawa zbierał dane w określonym celu, a następnie ustawodawca postanowił, że te dane mogą zostać wykorzystane w innym celu niż ten, który istniał w momencie zbierania danych. Realizacja indywidualnego obowiązku informacyjnego w stosunku do znacznej liczby osób (np. w przypadku bazy PESEL – wszystkich Polaków) znacznie utrudniałaby realizacje zadań publicznych.

Ponadto przykładowo administrator danych prowadzący postępowania administracyjne w formie papierowej będzie mógł skorzystać z przywołanego ograniczenia, aby nie

przeszukiwać kilkunastu tomów akt administracyjnych, aby stwierdzić, czy gdzieś przypadkiem nie znalazły się czyjeś dane osobowe, które nie były niezbędne dla postępowania administracyjnego.

Rozdział 2. Wyznaczenie inspektora ochrony danych. W Rozdziale 2 projektowanej ustawy uregulowano tryb notyfikacji inspektorów ochrony danych osobowych, zwanych dalej „inspektorami", oraz podmioty obowiązane w polskim porządku prawnym do wyznaczenia inspektora ochrony danych osobowych.

Rozporządzenie reguluje kwestię inspektorów w przepisach art. 37-39. Przypadki obligatoryjnego wyznaczenia inspektorów określa art. 37 Rozporządzenia. Zgodnie z tym przepisem administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze, gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę, lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

W innych niż ww. przypadkach wyznaczenie inspektora jest dobrowolne. Projektodawca nie zdecydował się rozszerzyć przedmiotowo sytuacji obligatoryjnego wyznaczania inspektora, traktując katalog wymieniony w art. 37 ust. 1 Rozporządzenia jako zapewniający dostateczną ochronę podmiotów danych, a jednocześnie uwzględniający także koszty powołania inspektora.

Rozporządzenie nie definiuje terminu „organu lub podmiotu publicznego". Grupa Robocza art. 29, jako unijne forum współpracy organów ochrony danych osobowych państw członkowskich UE, wskazała w swoich wytycznych, dotyczących inspektorów ochrony danych (WP243), że: „takie pojęcie powinno zostać określone na poziomie przepisów krajowych. Do podmiotów takich najczęściej zalicza się organy władzy krajowej, organy regionalne i lokalne, ale również – na mocy właściwego prawa krajowego - szereg innych

podmiotów prawa publicznego". Uwzględniając powyższe oraz treść Rozporządzenia, wskazującego na obowiązek wyznaczenia inspektorów, ciążący na „organach lub podmiotach publicznych", projektodawca zdecydował się wprowadzić do projektu szerokie rozumienie takich podmiotów publicznych. Przepisy projektu w celu zapewnienia stosowania art. 37 ust. 1 lit. a Rozporządzenia precyzują, iż organami i podmiotami publicznymi obowiązanymi do wyznaczenia inspektora są organy publiczne i podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, a także instytuty badawcze oraz Narodowy Bank Polski.

Kwalifikacje, jakie powinien posiadać inspektor, określono bezpośrednio w Rozporządzeniu. Z jego przepisów wynika, iż inspektor powinien dysponować wiedzą fachową na temat prawa oraz odbyć praktyki w dziedzinie ochrony danych, a także posiadać umiejętność wypełniania zadań, o których mowa w art. 39 Rozporządzenia. Projektodawca nie zdecydował się na dookreślenie kwalifikacji, jakie powinien spełniać inspektor, wychodząc z założenia, że każda próba doprecyzowania tych przesłanek - np. w zakresie długości praktyk - mogłaby narazić go na zarzut nakładania ograniczeń, niewystępujących w innych państwach członkowskich UE, a tym samym barierę w swobodzie świadczenia usług. Co do umiejętności wypełniania zadań, to należy podkreślić, iż odpowiedzialność za wybór inspektora, a tym samym za umiejętność wykonywania zadań, ponosi administrator. To w jego interesie leży taki wybór inspektora, który da mu rękojmię umiejętnego wykonywania przez niego zadań. Grupa Robocza art. 29 wskazała w swoich wytycznych nr WP 243, dotyczących inspektorów ochrony danych, że wymagany rozporządzeniem 2016/679 „poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych, przetwarzanych w ramach jednostki. Dla przykładu, w przypadku wyjątkowo skomplikowanych procesów przetwarzania danych osobowych lub w przypadku przetwarzania dużej ilości danych szczególnych kategorii, inspektor może potrzebować wyższego poziomu wiedzy i wsparcia. Ponadto inaczej sytuacja przedstawiać się będzie w przypadku podmiotów regularnie przekazujących dane do państw trzecich niż w przypadku, gdy przekazywanie takie ma charakter okazjonalny. W związku z tym wybór inspektora powinien być dokonany z zachowaniem należytej staranności i brać pod uwagę charakter przetwarzania danych w ramach podmiotu". Z kolei, wypowiadając się w przedmiocie kryterium kwalifikacji zawodowych, Grupa wskazała, że: „istotne jest, by inspektor posiadał odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość rozporządzenia. Propagowanie

odpowiednich i regularnych szkoleń dla inspektorów przez organy nadzorcze również może być przydatne. Przydatna jest również wiedza na temat danego sektora i podmiotu administratora. Inspektor powinien również posiadać odpowiednią wiedzę na temat operacji przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych. W przypadku organów i podmiotów publicznych Inspektor powinien również posiadać wiedzę w zakresie procedur administracyjnych i funkcjonowania jednostki". Powyższe stanowiska wskazują więc skuteczny kierunek wykładni przepisów Rozporządzenia i są praktycznym drogowskazem dla inspektorów (dzisiejszych Administratorów Bezpieczeństwa Informacji, zwanych dalej „ABI"). Jednocześnie należy wskazać, że w dzisiejszym porządku prawnym ustawodawca także nie wypowiada się w przedmiocie kwalifikacji zawodowych koniecznych do pełnienia funkcji ABI. Przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wskazują bowiem, że funkcję taką może pełnić osoba, posiadająca odpowiednią wiedzę w zakresie ochrony danych osobowych. Weryfikację takiego kryterium podejmuje więc w każdym przypadku przedsiębiorca zatrudniający ABI oraz Generalny Inspektor Ochrony Danych Osobowych na etapie przeprowadzanych postępowań kontrolnych.

Co ważne, projekt Rozporządzenia przewiduje, że inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. W tym miejscu należy zwrócić także uwagę, iż art. 37 Rozporządzenia nie przyznaje państwom członkowskim kompetencji do określenia, w ilu maksymalnie podmiotach dana osoba może pełnić funkcję inspektora.

Projektodawca nie zdecydował się przewidzieć w projektowanych przepisach instytucji zastępcy inspektora ochrony danych oraz możliwości powołania kilku inspektorów w jednym podmiocie. W opinii projektodawcy byłoby to niezgodne z Rozporządzeniem. Zgodnie z art. 37 oraz motywem 97 Rozporządzenia administrator i podmiot przetwarzający wyznaczają inspektora, mowa jest o inspektorze w liczbie pojedynczej. Co więcej ustawodawca unijny przewidział możliwość wyznaczenia jednego inspektora dla kilku podmiotów, nie przewidział natomiast możliwości wyznaczenia kilku inspektorów czy też zastępcy inspektora w jednym podmiocie. Ponadto warto zauważyć, że inspektorem może zostać osoba, która posiada odpowiednie kwalifikacje zawodowe oraz wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych, ponadto inspektor ma obowiązek m.in. współpracować z organem nadzorczym oraz pełnić funkcję punktu kontaktowego. Natomiast wyznaczenie zastępców wiąże się z prawem do delegowania uprawnień i obowiązków także

w sytuacji, gdy w danym podmiocie jest obecny inspektor. Na taką osobę mogłyby zostać przekazane niektóre zadania czy też uprawniania przysługujące inspektorowi. W opinii projektodawcy, w przypadku gdy administrator albo podmiot przetwarzający poweźmie wiadomość o długiej nieobecności inspektora ochrony danych osobowych, powinien on wyznaczyć nową osobę do pełnienia tej funkcji, o czym powinien niezwłocznie zawiadomić Prezesa Urzędu. W przypadku krótszej, okresowej nieobecności administrator bądź podmiot przetwarzający powinien upoważnić innego pracownika do podejmowania działań inspektora.

Rozdział 3. Warunki i tryb udzielania akredytacji podmiotowi certyfikującemu. Zgodnie z art. 42 ust. 1 Rozporządzenia państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, mających świadczyć o zgodności z Rozporządzeniem operacji przetwarzania, prowadzonych przez administratorów i podmioty przetwarzające.

Ministerstwo Cyfryzacji w związku z oceną podjętą w ramach przeprowadzanych konsultacji projektowanych przepisów zdecydowało się zmodyfikować projektowane regulacje w zakresie mechanizmów certyfikacji. Zgodnie z przepisami projektu ustawy o ochronie danych osobowych Prezes Urzędu będzie uprawniony do wydawania certyfikatów, ale do ich wydawania dopuszczeni zostaną również przedsiębiorcy. Celem odciążenia działań podejmowanych przez polski organ nadzorczy, kompetencja do akredytacji podmiotów certyfikujących przyznana została Polskiemu Centrum Akredytacji, będącego krajową jednostką akredytującą w rozumieniu art. 2 pkt 11 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30). W ocenie projektodawcy powyższe rozwiązania w pełni oddają intencję ustawodawcy unijnego towarzyszącą wprowadzeniu do unijnego porządku prawnego mechanizmu certyfikacji poprzez włączenie do mechanizmu certyfikacji nie tylko organu nadzorczego, ale również innych podmiotów. Z informacji uzyskanych w toku prowadzonych prac legislacyjnych od Komisji Europejskiej wynika, że przyznanie kompetencji do certyfikacji wyłącznie Prezesowi Urzędu budziłoby wątpliwości pod kątem zgodności z art. 42 ust. 5 rozporządzenia 2016/679, który mówi o tym, że certyfikacji dokonują podmioty certyfikujące lub właściwy organ nadzorczy.

Rozdział 4. Warunki i tryb dokonywania certyfikacji. Jak zostało to wskazane, zgodnie z przepisami projektu ustawy o ochronie danych osobowych Prezes Urzędu będzie uprawniony do wydawania certyfikatów, ale do ich wydawania dopuszczeni zostaną również przedsiębiorcy. Prowadzenie certyfikacji jest odrębnym działaniem niż pozostałe zadania Prezesa Urzędu, w tym zadania związane z prowadzeniem postępowań w sprawie naruszenia przepisów o ochronie danych, czy przeprowadzanie czynności kontrolnych.

Przepisy Rozporządzenia nie precyzują dokładnie zakresu możliwej certyfikacji. W szczególności możliwe było uznanie, że certyfikacji mogą podlegać administratorzy oraz podmioty przetwarzające, procesy przetwarzania danych osobowych bądź produkty, które w swoim założeniu mają w przyszłości służyć przetwarzaniu danych osobowych. Art. 42 Rozporządzenia wskazuje jedynie, że certyfikaty mają „świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające", nie wskazuje jednak, że ich adresatem mogą być wyłącznie administratorzy bądź podmioty przetwarzające. W świetle powyższego projektodawca zdecydował się ustanowić szeroki zakres certyfikacji, obejmując nim zarówno administratora, podmiot przetwarzający, producenta albo podmiot wprowadzający produkt na rynek. W ocenie projektodawcy doniosły wymiar certyfikacji w obszarze ochrony danych osobowych uzasadnia przyjęcie jednak jej szerokiego zastosowania poprzez objęcie mechanizmem certyfikacji nie tylko administratorów i podmiotów przetwarzających, ale również podmioty które produkują rozwiązania służące przetwarzaniu danych osobowych. Można bowiem wyobrazić sobie ogrom przypadków, w ramach których dany przedsiębiorca nie jest administratorem danych osobowych, ale tworzy systemy informatyczne bądź inne produkty, które w przyszłości będą służyły przetwarzaniu takich danych. Rozszerzenie mechanizmów certyfikacji na takie obszary nie tylko nie ogranicza zastosowania przepisów Rozporządzenia, ale je poszerza, wpływając na podwyższenie poziomu ochrony danych osobowych.

Certyfikacji dokonuje się na wniosek administratora lub podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek. Certyfikacji dokonuje się na podstawie kryteriów określonych przez Prezesa Urzędu. Jednym z zadań Rady do Spraw Ochrony Danych Osobowych, zwanej dalej „Radą", która jest organem opiniodawczo-doradczym, jest opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych, opiniowanie przekazanych przez Prezesa Urzędu projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych, opracowywanie propozycji kryteriów certyfikacji. Pozwoli to na

zachowanie dodatkowych warunków bezstronności zasad dokonywania certyfikacji przez Prezesa Urzędu.

Projektodawca zdecydował się uregulować wysokość opłaty pobieranej za czynności certyfikacyjne przez Prezesa Urzędu. Prezes Urzędu Ochrony Danych Osobowych będzie mógł pobierać za czynności związane z przeprowadzeniem certyfikacji opłatę maksymalną. W efekcie opłata przewidziana w projekcie stanowić będzie opłatę maksymalną za czynności prowadzone przez Prezesa Urzędu w celu dokonania certyfikacji i jej ewentualnego udzielenia wnioskodawcy. Proponowana zmiana w zależności od podmiotu, który ubiega się o certyfikację, oraz od zakresu dokonywanej certyfikacji pozwoli zróżnicować wysokość należnej opłaty, tak aby była ona akceptowalna dla małych podmiotów, w tym mikroprzedsiębiorstw. Prezes Urzędu na swojej stronie podmiotowej Biuletynu Informacji Publicznej będzie podawał wysokość opłaty, jaką podmiot ubiegający się o udzielenie certyfikacji obowiązany będzie ponieść z tytułu czynności związanych z certyfikacją.

Maksymalna wysokość opłaty została określona w ustawie jako kwota odpowiadająca czterokrotności przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok złożenia wniosku o certyfikację, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2017 r. poz. 1383, 1386, 2120 oraz z 2018 r. poz. 138).

Projektodawca nie zdecydował się na uregulowanie wysokości opłaty za akredytację podejmowaną przez Polskie Centrum Akredytacji, determinowanej przez inne przepisy powszechnie obowiązującego prawa, wiążące Polskie Centrum Akredytacji.

W ocenie projektodawcy bardzo ważnym jest, aby podmiot certyfikujący podejmował swoje działania bez narażenia się na konflikt interesów. Jest to standard obowiązujący na rynku podmiotów świadczących usługi certyfikacyjne w różnych branżach i sektorach. W szczególności niedopuszczalnym w ocenie projektodawcy byłaby sytuacja, w której certyfikacja podejmowana byłaby przez podmiot certyfikujący wobec podmiotów będących w chwili certyfikacji bądź kiedyś klientami podmiotu certyfikującymi w zakresie porad prawnych dotyczących ochrony danych osobowych.

Rozdział 5. Opracowywanie i zatwierdzanie kodeksu postępowania oraz warunki i tryb akredytacji podmiotu monitorującego jego przestrzeganie. Przepisy rozdziału 5 projektu dotyczą monitorowania przestrzegania zatwierdzonego kodeksu postępowania, o którym

mowa w art. 40 Rozporządzenia. Przepis ten stanowi m.in., iż państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia - z uwzględnieniem specyfiki różnych sektorów, dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz MŚP (Małych i Średnich Przedsiębiorstw). Zrzeszenia i inne podmioty, reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie niniejszego rozporządzenia. Projekt nowej ustawy przewiduje, iż monitorowaniem przestrzegania zatwierdzonego kodeksu postępowania będą zajmowały się podmioty akredytowane przez Prezesa Urzędu.

Prezes Urzędu będzie udostępniał wykaz podmiotów akredytowanych w Biuletynie Informacji Publicznej. Projektodawca przykłada szczególne znaczenie do możliwej, pełnej transparentności procesu tworzenia kodeksów postępowania. W szczególności zgodnie z motywem 99 preambuły do Rozporządzenia, „sporządzając kodeks postępowania bądź zmieniając go lub rozszerzając jego zakres, zrzeszenia i inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających powinny konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą, oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji". Projektodawca nie chciał ograniczyć zakresu podmiotów uczestniczących w konsultacjach wyłącznie do określonej kategorii podmiotów, jak organizacje społeczne bądź podmioty reprezentujące kategorie administratorów, jak izby gospodarcze. W świetle powyższego, projekt nakłada ogólny obowiązek konsultacji tworzonych kodeksów z zainteresowanymi podmiotami.

Rozdział 6. Prezes Urzędu Ochrony Danych Osobowych. Rozdział zawiera kluczową regulację ustrojową – przepisy dotyczące Prezesa Urzędu Ochrony Danych Osobowych. Przepis art. 8 obowiązującej Ustawy stanowi, że organem do spraw ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych. Przepisy projektowanej ustawy ustanawiają nowy organ właściwy w sprawie ochrony danych osobowych, będzie nim Prezes Urzędu Ochrony Danych Osobowych. Zgodnie z motywem 117 Rozporządzenia „zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, uprawnionych do wypełniania zadań i wykonywania uprawnień w sposób całkowicie

niezależny". Każde z państw członkowskich w świetle przyznanej im zasady autonomii instytucjonalnej oraz proceduralnej może ustanowić więc niezależny aparat państwowy, nadzorujący przestrzeganie przepisów Rozporządzenia. Ponieważ uchylona zostaje podstawa prawna działania Generalnego Inspektora Ochrony Danych Osobowych – co jest konieczne w celu wydania aktu zapewniającego skuteczne stosowanie Rozporządzenia, a obowiązująca Ustawa implementuje uchylaną dyrektywę, nowy organ nadzorczy z prawnego punktu widzenia jest nowym organem państwowym, będącym następcą prawnym Generalnego Inspektora.

Do nadania organowi nadzorczemu nazwy Prezesa Urzędu Ochrony Danych Osobowych skłoniła Projektodawcę treść przepisów Rozporządzenia, a decyzja w tym zakresie ma wyłącznie wymiar porządkujący. Po pierwsze, Rozporządzenie wprowadza funkcję „inspektora ochrony danych" jako osoby fizycznej wyznaczanej przez administratora bądź podmiot przetwarzający wewnątrz ich struktury organizacyjnej i obowiązanej do szeroko rozumianego monitorowania przestrzegania Rozporządzenia. Jednocześnie brak jest jednak jakiegokolwiek związku ustrojowego pomiędzy takimi osobami a przyszłym organem nadzorczym, odpowiadającym za egzekwowanie w Polsce przestrzegania przepisów Rozporządzenia. Przyjęcie obecnej nazwy organu wprowadzałoby w tym zakresie w błąd, w tym co do ich pozycji ustrojowej. Zgodnie bowiem z art. 38 ust. 3 Rozporządzenia inspektorzy ochrony danych muszą być niezależni. Po drugie utrzymanie obecnej nazwy - Generalny Inspektor Ochrony Danych Osobowych powodowałoby niejako konieczność nazwania inspektorami pracowników biura, którzy w imieniu organu przeprowadzają postępowanie kontrolne. Skoro bowiem mamy Generalnego Inspektora, muszą funkcjonować w jego strukturze organizacyjnej inni inspektorzy, względem których jest on inspektorem generalnym (tak jak ma to miejsce na kanwie obowiązujących przepisów). Powyższe przesądziłoby z kolei, że w systemie ochrony danych osobowych mielibyśmy dwie kategorie inspektorów – pracowników organu nadzorczego oraz osoby mające zupełnie inny status powoływane wewnątrz struktury organizacyjnej administratorów i podmiotów przetwarzających, co jest w ocenie projektodawcy niedopuszczalne. Uwzględniając powyższe, odstąpiono również od nazywania pracowników organu nadzorczego przeprowadzających w jego imieniu czynności kontrolne inspektorami na rzecz nazwania ich kontrolującymi. Projektodawca, nadając organowi nazwę Prezesa Urzędu Ochrony Danych Osobowych, dokonał wyczerpującej analizy nazewnictwa wykorzystywanego w Polsce względem innych organów państwowych. Uwagę należy w tym zakresie zwrócić chociażby

na Państwową Inspekcję Pracy i działających w jej ramach inspektorów pracy oraz społecznych inspektorów pracy. Po pierwsze bowiem podmioty takie działają na zupełnie innej podstawie prawnej. O ile podstawą prawną działań podejmowanych przez inspektorów pracy jest ustawa z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy (Dz. U. z 2018 r. poz. 623), o tyle podstawą działań podejmowanych przez społecznych inspektorów pracy jest ustawa z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy (Dz. U. z 2015 r. poz. 567). Po drugie, z uwagi na zakres zadań prowadzonych przez społecznych inspektorów pracy, przepisy nie podkreślają ich niezależności, jak ma to miejsce w Rozporządzeniu. Wręcz przeciwnie, zgodnie z art. 18 ustawy o społecznej inspekcji pracy, Państwowa Inspekcja Pracy udziela pomocy społecznej inspekcji pracy w realizacji jej zadań, w szczególności przez poradnictwo prawne, specjalistyczną prasę oraz szkolenie. Inspektorzy pracy Państwowej Inspekcji Pracy przeprowadzają kontrole wykonania zaleceń i uwag społecznych inspektorów pracy. Pomiędzy Państwową Inspekcją Pracy i społecznymi inspektorami pracy istnieje więc związek, którego brak jest w przypadku niezależnych względem organu nadzorczego inspektorów ochrony danych. Wreszcie celem wyeliminowania wszelkich wątpliwości, społecznym inspektorom pracy nadano właśnie nazwę „społecznych inspektorów pracy", a nie „inspektorów pracy", by odróżnić ich od pracowników organu – czego nie można zrobić w przepisach zapewniających skuteczne stosowanie Rozporządzenia. Uwzględniając powyższe oraz doręczane Ministrowi Cyfryzacji różne postulaty, w tym od stowarzyszeń skupiających administratorów bezpieczeństwa informacji, najwłaściwszym jest użycie nazwy wykorzystywanej w Polsce najczęściej i najłatwiejszej do przyswojenia dla obywateli – Prezes Urzędu Ochrony Danych Osobowych. W trakcie prowadzonych prekonsultacji rozwiązanie takie zostało również poparte przez znaczną część izb gospodarczych oraz stowarzyszeń reprezentujących interesy administratorów bezpieczeństwa informacji.

Przepisy projektowanej ustawy stawiają zgodnie z wymogami przewidzianymi w Rozporządzeniu wysokie wymogi Prezesowi Urzędu. W szczególności przewiduje, że musi on wyróżniać się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych.

Z uwagi na ogromne doświadczenie w sprawowaniu nadzoru nad ochroną danych osobowych przez Generalnego Inspektora Ochrony Danych Osobowych założeniem jest zapewnienie faktycznej ciągłości działania organu. W związku z powyższym, z dniem wejścia w życie ustawy pracownicy zatrudnieni w Biurze Generalnego Inspektora Ochrony Danych Osobowych stają się pracownikami Urzędu Ochrony Danych Osobowych, mienie Skarbu

Państwa będące we władaniu Biura Generalnego Inspektora Ochrony Danych Osobowych staje się mieniem będącym we władaniu Urzędu Ochrony Danych Osobowych, a należności i zobowiązania Biura Generalnego Inspektora Ochrony Danych Osobowych z dniem wejścia w życie ustawy stają się należnościami i zobowiązaniami Urzędu Ochrony Danych Osobowych.

Organ zgodnie z projektem będzie powoływany przez Sejm Rzeczypospolitej Polskiej za zgodą Senatu Rzeczypospolitej Polskiej. Organ będzie również na etapie jego powoływania składał ślubowanie przed Sejmem Rzeczypospolitej Polskiej, dysponując również immunitetem formalnym. Kandydat na stanowisko Prezesa Urzędu będzie musiał spełnić kryterium wyższego wykształcenia, wiedzy i doświadczenia z zakresu ochrony danych osobowych.

Prezes Urzędu będzie organem kadencyjnym, odwołalnym w wyjątkowych, wynikających z Rozporządzenia przypadkach. Zgodnie z art. 53 ust. 4 Rozporządzenia „członek organu nadzorczego może zostać odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki niezbędne do pełnienia obowiązków". Celem wzmocnienia niezależności organu nadzorczego, projektodawca zdecydował się wskazać, m. in. że odwołanie możliwe jest nie tylko w razie poważnego uchybienia, ale tylko gdy takie uchybienie zostało stwierdzone prawomocnym wyrokiem sądu i polegało na popełnieniu umyślnego przestępstwa lub umyślnego przestępstwa skarbowego. Pozostałe przypadki to m.in. sprzeniewierzenie się złożonemu ślubowaniu oraz pozbawienie praw publicznych.

Wzmocnieniu pozycji organu nadzorczego służyć mają również takie projektowane instrumenty jak przyznanie organowi prawa do przeprowadzania kontroli naruszenia zasad ochrony danych osobowych czy możliwość korzystania z pomocy funkcjonariuszy Policji w toku przeprowadzanej kontroli. Organ sam będzie również decydował o nadawaniu sobie statutu – obecnie robi to Prezydent Rzeczypospolitej Polskiej. Jednocześnie należy wskazać, że utrzymana zostanie pozycja ustrojowa organu, jako podlegającego wyłącznie ustawie, kadencyjnego i nienależącego do administracji rządowej. Projektodawca w związku z przeprowadzonymi konsultacjami społecznymi zdecydował się ostatecznie nie zmieniać w żadnym zakresie procedury powołania organu – względem aktualnie obowiązujących regulacji.

W celu zapewnienia realizacji zadań nakładanych na nowy organ właściwy w sprawie ochrony danych osobowych oraz wzmocnienia jego pozycji przewidziano możliwość

powołania do trzech zastępców Prezesa Urzędu. Rozwiązanie takie podyktowane jest bardzo szerokim zakresem zadań nałożonych na Prezesa Urzędu, które często wymagają innych kwalifikacji. Jako przykład można w tym zakresie podać wymóg prowadzenia współpracy międzynarodowej, podejmowania działań certyfikacyjnych, podejmowania działań edukacyjnych, prowadzenia postępowań w sprawach naruszenia przepisów o ochronie danych czy nadzoru nie tylko nad Rozporządzeniem, ale również tzw. dyrektywą policyjną. Każde z tych działań może być przykładowo wspierane przez innego zastępcę Prezesa Urzędu.

Należy w szczególności wskazać, że wprowadzenie zmian w procedurze powołania zastępców Prezesa Urzędu względem procedury obowiązującej obecnie w przypadku Generalnego Inspektora Ochrony Danych Osobowych ma na celu wzmocnienie niezależności organu. Po pierwsze bowiem, obowiązujące obecnie przepisy prawne przewidują, że odwołania zastępcy może dokonać Marszałek Sejmu na wniosek GIODO. Powyższe oznacza, że Marszałek Sejmu nie jest związany wnioskiem GIODO i może odmówić odwołania zastępcy GIODO. Projektowana regulacja przewiduje, że odwołania zastępcy Prezesa Urzędu dokonuje Prezes Urzędu bez konieczności podejmowania w tym zakresie jakiejkolwiek konsultacji z innym organem. Po drugie, przepisy wskazują wyraźnie, że to Prezes Urzędu powołuje swoich zastępców, a nie tak jak obecnie inny organ państwowy – w obowiązującej ustawie Marszałek Sejmu. Wreszcie po trzecie, w przypadku powołania przez Prezesa Urzędu jakiegokolwiek zastępcy, będzie swobodny w odwołaniu ich. W świetle obowiązujących obecnie przepisów ustawy, GIODO swobody takiej nie ma.

Wreszcie nową instytucją powoływaną przez Prezesa Urzędu ma być Rada do Spraw Ochrony Danych Osobowych. W ocenie projektodawcy szeroki zakres zadań Prezesa Urzędu oraz potrzeba stałej grupy osób wspomagających Prezesa Urzędu w realizacji jego zadań uzasadniają powołanie przy Prezesie Urzędu organu opiniodawczo-doradczego. Skład Rady został tak zaprojektowany, by mogły do niego wchodzić osoby reprezentujące różne podmioty, zarówno ze strony administracji publicznej, jak i spoza administracji. Ideą jest, by różne podmioty mogły wesprzeć swoją wiedzą Prezesa Urzędu. Przepisy projektu stanowią o sprawozdaniach składanych przez Prezesa Urzędu i służą zapewnieniu stosowania art. 59 Rozporządzenia.

Projekt nadaje Prezesowi Urzędu uprawnienie do opiniowania założeń i projektów aktów prawnych dotyczących danych osobowych. Z przepisu § 38 ust. 1 Regulaminu pracy Rady Ministrów wynika natomiast obowiązek kierowania przez organy wnioskujące projektów dokumentów rządowych do zaopiniowania przez organy administracji rządowej lub inne

organy i instytucje państwowe, których zakresu działania dotyczy projekt. Celem przepisu art. 36 projektu jest zapewnienie stosowania art. 57 ust. 1 lit. c Rozporządzenia.

Projekt zawiera też powielenie rozwiązań funkcjonujących i sprawdzających się na gruncie obowiązującej Ustawy, zgodnie z którymi Prezes Urzędu może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Przepisy dotyczą udostępniania przez Prezesa Urzędu w Biuletynie Informacji Publicznej standardowych klauzul umownych i zatwierdzonych kodeksów postępowania i służą wskazaniu sposobu podawania do publicznej wiadomości ww. dokumentów.

Projekt ma na celu określenie formy prawnej podawania przez Prezesa Urzędu do wiadomości publicznej wykazu rodzajów operacji przetwarzania danych osobowych podlegających wymogowi dokonania oceny skutków dla ochrony danych. Przyjmuje się, iż wykaz ten będzie często aktualizowany, stąd forma jego ogłoszenia musi umożliwiać jego bieżącą aktualizację.

Projekt nakłada na Prezesa Urzędu obowiązek opracowywania i udostępniania rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Zgodnie z art. 32 ust. 1 Rozporządzenia, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Ww. regulacja jest wyrazem zastosowania w Rozporządzeniu podejścia *risk based approach*, a więc podejścia opartego na ryzyku administratora lub podmiotu przetwarzającego. To już nie przepisy prawa powszechnie obowiązującego mają określać środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, ale sami administratorzy lub podmioty przetwarzające. Stosowane środki powinny być zawsze dostosowane do okoliczności i ryzyk związanych z przetwarzaniem danego rodzaju danych osobowych. Tym

niemniej, w ocenie projektodawcy, by zapewnić administratorom i podmiotom przetwarzającym wsparcie w określaniu takich środków, uzasadnione jest, by Prezes Urzędu opracowywał i udostępniał rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Rekomendacje takie powinny być wypracowane przy współpracy z zainteresowanymi podmiotami, których zakresu działania dotyczy dany projekt – w tym z izbami gospodarczymi. Rekomendacje nie będą miały mocy wiążącej, ale będą stanowiły punkt odniesienia dla przedsiębiorców, wpływając w ocenie projektodawcy na podwyższenie poziomu ochrony danych osobowych.

Prezes Urzędu jest organem uprawnionym do prowadzenia dużej liczby postępowań. Dla celów porządkowych należy wskazać, że w przypadku postępowania w sprawach naruszenia przepisów o ochronie danych osobowych, w sprawach nieuregulowanych w ustawie do postępowania przed Prezesem Urzędu stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Do procedury zawiadomienia, zmiany danych i odwołania przez Prezesa Urzędu wyznaczenia przez administratora albo podmiot przetwarzający inspektora ochrony danych osobowych, do procedury akredytacji podmiotów certyfikujących nie stosuje się przepisów Kodeksu postępowania administracyjnego.

Rozdział 7. Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych. Przepisy rozdziału 7 projektu ustawy regulują sposób postępowania w sprawach naruszenia przepisów o ochronie danych osobowych. Należy przede wszystkim podkreślić, iż, mówiąc o naruszeniu przepisów o ochronie danych osobowych, projektodawca odnosi się nie tylko do naruszeń ustawy, ale również przepisów Rozporządzenia, z których w sposób bezpośredni wynikają określone prawa i obowiązki podmiotów danych osobowych, administratorów lub podmiotów przetwarzających.

Na gruncie obowiązującej Ustawy postępowanie w sprawach naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", prowadzi się według przepisów Kodeksu postępowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej. Zasada stosowania w sprawach nieuregulowanych Kodeksu postępowania administracyjnego, dalej również „k.p.a.", została zachowana w projekcie. Projektodawca nie zdecydował się na wprowadzenie odrębnego, właściwego dla naruszeń ochrony danych osobowych, trybu postępowania przed Prezesem Urzędu. U podstaw takiej decyzji legło przekonanie, iż obowiązująca procedura administracyjna, z odmiennościami wynikającymi choćby z bezpośredniego stosowania Rozporządzenia, zapewnia kompletny, a zarazem sprawdzony w

praktyce mechanizm postępowania. Postępowania prowadzone przez Prezesa Urzędu będą postępowaniami w sprawie naruszenia prawa podstawowego, a stronom tak prowadzonych postępowań przysługiwać powinien pełen katalog uprawnień procesowych przewidzianych w k.p.a. Wyłączenie stosowania k.p.a. i próba stworzenia szczególnego postępowania w sprawie naruszenia przepisów o ochronie danych obarczona byłaby, z jednej strony, ryzykiem nieuregulowania niezbędnych elementów postępowania, a z drugiej, koniecznością tworzenia obszernej listy przepisów k.p.a., które jednak znalazłyby zastosowanie w tym postępowaniu. Działania takie uznano za niepropocjonalne. Postępowanie będzie prowadzone przez Prezesa Urzędu jako organ właściwy w sprawie ochrony danych osobowych. Korzystając z możliwości przewidzianej w Konstytucji RP oraz w k.p.a., projektodawca przewidział jednoinstancyjność postępowania. Odnosząc się do projektowanego rozwiązania, należy zauważyć, że konstytucyjna zasada zaskarżalności orzeczeń i decyzji wydanych w pierwszej instancji „(...) obejmuje swym zakresem nie tylko postępowanie sądowe, ale również administracyjne oraz inne postępowania, w których organ władzy publicznej wydaje akt kształtujący sytuację prawną podmiotu praw i wolności" (wyrok TK z dnia 6 grudnia 2011 r. SK 3/11). Jednocześnie zasada dwuinstancyjności nie ma charakteru absolutnego, na co wskazuje sam art. 78 zdanie drugie Konstytucji, a zatem ustawodawca może wprowadzać wyjątki od tej zasady, wprowadzając określone postępowanie jednoinstancyjnym. Zasady ustanawiania takich wyjątków nakreślił Trybunał Konstytucyjny, m.in. w uzasadnieniu wyroku z dnia 12 czerwca 2002 r., P 13/01, wskazując, że: „Powinny być one ustalone w ustawie. Konstytucja nie precyzuje charakteru tych wyjątków, nie wskazuje bowiem ani zakresu podmiotowego, ani przedmiotowego, w jakim odstępstwo od tej zasady jest dopuszczalne. Nie oznacza to jednak, iż ustawodawca ma pełną, niczym nieskrępowaną swobodę w ustalaniu katalogu takich wyjątków. W pierwszym rzędzie należy liczyć się z tym, iż nie mogą one prowadzić do naruszenia innych norm konstytucyjnych. (...) [ponadto] odstępstwo od reguły wyznaczonej treścią normatywną art. 78 Konstytucji w każdym razie powinno być podyktowane szczególnymi okolicznościami, które usprawiedliwiałyby pozbawienie strony postępowania środka odwoławczego". Zgodnie z dominującym stanowiskiem Trybunału wyjątki od zasady dwuinstancyjności powinny również czynić zadość wymaganiom stawianym przez zasadę proporcjonalności (art. 31 ust. 3 Konstytucji; wyroki TK: z dnia 17 lutego 2004 r., SK 39/02; z dnia 18 kwietnia 2005 r., SK 6/05; z dnia 14 października 2010 r., K 17/07).

Przewidziany przez projektodawcę wyjątek od zasady dwuinstancyjności postępowania administracyjnego jest, w jego ocenie, konieczny w demokratycznym państwie dla zapewnienia wolności i praw osób. Jest to rozwiązanie adekwatne i konieczne dla osiągnięcia celu zamierzonego przez ustawodawcę, jakim jest skuteczna i udzielona we właściwym czasie ochrona prawa podstawowego - prawa do ochrony danych osobowych osoby fizycznej, oraz pozostaje w odpowiedniej proporcji do ograniczenia, jakim jest pozbawienie prawa do ponownego rozpatrzenia sprawy przez właściwy organ. Za wprowadzeniem jednoinstancyjności postępowania przemawia konieczność zapewnienia osobie, której prawa zostały naruszone, ostatecznego rozstrzygnięcia (ostatecznej decyzji administracyjnej), które będzie mogło być skutecznie i szybko egzekwowalne. Tak więc w ocenie projektodawcy ochrona danych osobowych osoby fizycznej wymaga, by zasadą była natychmiastowa wykonalność takich decyzji. Ochrona wartości, jaką są dane osobowe osoby fizycznej, wymaga natychmiastowego działania, inaczej często traci swój sens, gdyż z upływem czasu naruszenia mogą mieć miejsce na wielką skalę, a ich skutki nieodwracalny charakter.

Warto również podkreślić, że w postępowaniu prowadzonym przez Prezesa Urzędu nie mamy do czynienia z odwołaniem składanym do organu wyższego stopnia, lecz z wnioskiem o ponowne rozpatrzenie sprawy, który rozpatrywany jest przez ten sam organ. Jak pokazują statystyki dotyczące decyzji wydawanych w postępowaniach w wyniku wniosku o ponowne rozpatrzenie sprawy, decyzje wydawane po ponownym rozpatrzeniu sprawy w zdecydowanej większości nie prowadzą do zmiany rozstrzygnięć wydawanych w pierwszej instancji przez organ właściwy w sprawie ochrony danych osobowych.

Należy podkreślić, iż rozstrzygnięcia wydawane przez Prezesa Urzędu jako organ właściwy w sprawie ochrony danych osobowych będą podlegały zaskarżeniu do sądu administracyjnego i skargi w tych sprawach będą podlegały dwuinstancyjnemu postępowaniu sądowoadministracyjnemu. Powyższe oznacza, iż prawa podmiotów danych osobowych i innych stron postępowania przed Prezesem Urzędu do wnikliwego rozpatrzenia sprawy i sądowej kontroli rozstrzygnięć administracji zostaną zapewnione. Nie zostaje również wyłączone prawo strony takiego postępowania do żądania wstrzymania wykonalności decyzji lub postanowienia.

Wprowadzenie zasady jednoinstancyjności postępowania służy realizacji celów zakładanych przez ustawodawcę, jakimi są zapewnienie adekwatnej i skutecznej ochrony praw osób, których prawo do ochrony danych osobowych zostało naruszone, i cele te są uzasadnione w świetle wartości wymienionych w art. 31 ust. 3 Konstytucji. Jednoinstancyjność postępowania

nie narusza bowiem prawa strony postępowania do kontroli rozstrzygnięcia wydawanego przez Prezesa Urzędu, nie narusza zatem istoty prawa, jaką jest konieczność ponownego, wnikliwego, niezależnego zbadania jej sprawy. W ocenie projektodawcy wprowadzenie ww. zasady jest niezbędne dla ochrony wartości, jaką jest prawo do ochrony danych osobowych, i nie można uznać jej wprowadzenia, biorąc pod uwagę ww. argumenty, za środek nadmiernie „restrykcyjny". Efekt wprowadzenia omawianej regulacji, a więc zapewnienie skutecznej ochrony podmiotom danych osobowych polegającej choćby na zatrzymaniu nieuprawnionego przekazywania danych osobowych osoby fizycznej do państw trzecich ma wartość większą niż wartość wynikająca z ponownego rozpatrzenia sprawy przez ten sam organ administracyjny. Należy wreszcie wskazać, że projektodawca zdecydował się wprowadzić do projektu „jednoinstancyjność" postępowania mimo brzmienia art. 127a k.p.a. Zgodnie z treścią rzeczonego artykułu w trakcie biegu terminu do wniesienia odwołania strona może zrzec się prawa do wniesienia odwołania wobec organu administracji publicznej, który wydał decyzję. W ocenie projektodawcy nawet treść takiego artykułu nie wyeliminowuje przypadków, w których jedna ze stron chociażby celem przedłużenia postępowania zdecyduje się złożyć odwołanie. Uwzględniając charakter ochrony danych osobowych jako prawa podstawowego, działanie takie w ocenie projektodawcy mogłoby pociągnąć za sobą poważne konsekwencje.

Obok jednoinstancyjności kolejną odrębnością postępowania przewidzianego w ustawie w stosunku do postępowania unormowanego w K.p.a. jest wskazanie, że w sprawach związanych z ochroną danych osobowych pełnomocnikiem może być przedstawiciel organizacji, do której zadań statutowych należą sprawy związane z ochroną danych osobowych. Powyższa regulacja ma na celu zapewnienie stosowania art. 80 Rozporządzenia. Powołany przepis nakłada na państwa członkowskie obowiązek przewidzenia w przepisach prawnych rozwiązania, w świetle którego organizację lub zrzeszenie – które nie ma charakteru zarobkowego i ma cele statutowe leżące w interesie publicznym i działa w dziedzinie ochrony danych osobowych – można umocować do wniesienia w jej imieniu skargi oraz wykonywania w jej imieniu praw. Zgodnie z treścią motywu 142 preambuły do Rozporządzenia, „jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z niniejszego rozporządzenia, powinna mieć ona prawo zlecić podmiotowi, organizacji lub zrzeszeniu wniesienie skargi w swoim imieniu do organu nadzorczego, wykonanie prawa do środka ochrony prawnej przed sądem w imieniu osób, których dane dotyczą, lub – o ile taką możliwość przewiduje prawo państwa członkowskiego – żądanie

odszkodowania w imieniu osób, których dane dotyczą". W projekcie ustawy wskazano, że organizacja społeczna, o której mowa w art. 31 § 1 k.p.a., może również występować w postępowaniu za zgodą osoby, której dane dotyczą, w jej imieniu i na jej rzecz osoby. Projektowana regulacja nie stanowi jednak przeszkody dla skorzystania przez stronę z osoby pełnomocnika, o którym mowa w art. 32 K.p.a.

W projekcie ustawy wprowadzono również rozwiązanie, zgodnie z którym Prezes Urzędu, zawiadamiając strony o niezałatwieniu sprawy w terminie, obowiązany jest również poinformować o stanie sprawy i przeprowadzonych w jej toku czynnościach. Należy wskazać, że powołana regulacja uzupełnia art. 36 k.p.a. i służy zapewnieniu pełnego stosowania art. 78 ust. 2 Rozporządzenia, który stanowi, iż bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 55 i art. 56 Rozporządzenia nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej do organu nadzorczego. Przyjmując, iż zgodnie z k.p.a. rozpatrzenie sprawy szczególnie skomplikowanej powinno nastąpić nie później niż w terminie dwóch miesięcy od dnia wszczęcia postępowania, a o każdym przypadku jej niezałatwienia w terminie należy zawiadomić strony, przyjęto, iż powyższa regulacja projektu zapewni stronie postępowania, w terminie trzech miesięcy od dnia wszczęcia postępowania, informację o postępach lub efektach rozpatrywania wniosku przed Prezesem Urzędu. Brak takiej informacji w terminie trzech miesięcy od dnia wszczęcia postępowania dawał będzie stronie prawo do wniesienia skargi do sądu administracyjnego. W ocenie projektodawcy państwo członkowskie, wzmacniając ochronę danych osobowych, może w praktyce zobowiązać organ nadzorczy do informowania osób, których dane dotyczą, wcześniej niż po upływie trzech miesięcy, a okres wynikający z Rozporządzenia jest okresem maksymalnym.

Projektowany przepis art. 64 służy zapewnieniu stosowania art. 90 Rozporządzenia. Jego celem jest wskazanie wprost w przepisie ustawy, że uprawnienia Prezesa Urzędu podlegają ograniczeniom w zakresie dostępu do informacji ustawowo chronionych. Odnosząc się do brzmienia art. 90 ust. 1 Rozporządzenia, uznano za niezbędne i proporcjonalne dla pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy ograniczenie uprawnień Prezesa Urzędu w odniesieniu do informacji, w tym danych osobowych, ustawowo chronionych. W związku z powyższym, zakres dostępu Prezesa Urzędu do informacji ustawowo chronionych będzie determinowany każdorazowo przepisami

obejmującymi informacje chronione. W ocenie projektodawcy z uwagi na możliwe ryzyko wykładni art. 58 Rozporządzenia w związku z art. 90 Rozporządzenia, zgodnie z którą w braku wyraźnej regulacji krajowej organ nadzorczy jest uprawniony do korzystania z uprawnień określonych w art. 58 ust. 1 lit. e i f Rozporządzenia, tj. uzyskiwania dostępu do danych osobowych i informacji, a także pomieszczeń i urządzeń niezbędnych do realizacji zadań organu nadzorczego, bez względu na obowiązek podmiotu kontrolowanego do zachowania tajemnicy, wynikający z regulacji sektorowych, postanowiono o wprowadzeniu do projektu właściwych przepisów. Z rozporządzenia nie wynika bowiem w sposób wyraźny zakaz korzystania z ww. uprawnień organu nadzorczego w zakresie, w jakim ich realizacja mogłaby być sprzeczna z ochroną tajemnic sektorowych.

Na gruncie Rozporządzenia wydaje się, że uprawnienia te nie doznają ograniczeń, a relacja rozporządzenia do krajowych regulacji tajemnic sektorowych może być różnie interpretowana. W ocenie projektodawcy przepis art. 90 Rozporządzenia należy rozumieć w ten sposób, że państwa członkowskie mogą ukształtować uprawnienia organu nadzorczego, o których mowa w art. 58 ust. 1 lit. e i f, ze względu na tajemnice zawodowe lub inne obowiązki równoważne zachowaniu tajemnicy, jeśli jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy. Państwa członkowskie mogą zatem uprawnienia przysługujące organowi nadzorczemu na podstawie art. 58 ust. 1 lit. e i f ograniczyć lub wyłączyć. Taka interpretacja przepisu art. 90 jest w ocenie projektodawcy zgodna z celem tego przepisu i motywem 164, które mają na celu przede wszystkim umożliwienie państwom członkowskim zapewnienia w przepisach krajowych ochrony tajemnic zawodowych. W ocenie projektodawcy proponowane przepisy pozostają w pełnej zgodności z rozporządzeniem 2016/679. Dostęp organu nadzorczego do informacji objętych tajemnicami odbywać się będzie w trybie, w zakresie i na zasadach przewidzianych w przepisach regulujących poszczególne tajemnice. Dane osobowe nie są bowiem wartością absolutną i ich ochrona nie może odbywać się kosztem narażenia na ujawnienie informacji chronionych szczególnymi reżimami. Projektowana ustawa powinna natomiast wyraźnie stanowić, że organ nadzorczy nie jest uprawniony do korzystania z uprawnień określonych w art. 58 ust. 1 lit. e i f Rozporządzenia w zakresie, w jakim informacje, które mogłyby zostać ujawnione w toku wykonywania czynności, w ramach postępowania, podlegają ochronie jako tajemnica zawodowa. Ewentualny dostęp organu nadzorczego do informacji objętych tajemnicami sektorowymi powinien się odbywać w trybie, zakresie i na zasadach przewidzianych w przepisach regulujących poszczególne

tajemnice. Dane osobowe nie są bowiem wartością absolutną i ich ochrona nie może odbywać się kosztem narażenia na ujawnienie informacji chronionych szczególnymi reżimami ochronnymi poza szczególnie uzasadnionymi przypadkami.

Przepisy projektu odnoszą się też do możliwości zastrzeżenia informacji, dokumentów lub ich części zawierających tajemnicę przedsiębiorstwa oraz ograniczenia prawa wglądu do materiału dowodowego. Zastrzeżenie tajemnicy przedsiębiorstwa nie ma charakteru bezwzględnego. Prezes Urzędu może je uchylić, jeśli nie są spełnione przesłanki uznania danej informacji za tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2018 r. poz. 419). Powyższa regulacja ma na celu zapewnienie ochrony tych informacji, które w ocenie strony postępowania będącego przedsiębiorcą mają charakter informacji technicznych, technologicznych, organizacyjnych lub też innych posiadających wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Projektodawca zdecydował się jednak nałożyć na przedsiębiorców obowiązek dostarczenia Prezesowi Urzędu wersji dokumentu niezawierającej informacji objętych zastrzeżeniem. W przypadku niedostarczenia wersji dokumentu niezawierającej informacji objętych zastrzeżeniem, zastrzeżenie uważa się za nieskuteczne. Projektowane rozwiązanie ma w swojej istocie wzmocnić potrzebę ochrony informacji objętych tajemnicą przedsiębiorstwa, uznając, że to przedsiębiorcy ustanawiający taką tajemnicę najlepiej potrafią ocenić jej zakres w każdym stanie faktycznym. Proponowane przepisy należy również oceniać w świetle przyznanych stronom uprawnień wglądu do akt sprawy, co wiąże się bardzo często z koniecznością usuwania z ich treści informacji objętych takimi tajemnicami, narażając organ na znaczne obciążenia.

Odnosząc się do ograniczenia prawa wglądu do materiału dowodowego, należy podkreślić, że może ono nastąpić tylko wtedy, jeśli groziłoby ujawnieniem tajemnicy przedsiębiorstwa lub innych tajemnic prawnie chronionych. Ograniczenie takie może nastąpić tylko na skutek postanowienia Prezesa Urzędu. Celem przepisu jest zapewnienie należytej ochrony tajemnicom ustawowo chronionym przy jednoczesnym badaniu w każdym przypadku przez Prezesa Urzędu zasadności ograniczenia dostępu do materiału dowodowego ze względu na te tajemnice.

Przepis stanowi modyfikację przepisu art. 88 K.p.a. Celem tego przepisu jest zwiększenie wysokości grzywny za niestawienie się bez uzasadnionej przyczyny jako świadek lub biegły albo bezzasadne odmówienie złożenia zeznania, wydania opinii, okazania przedmiotu

oględzin albo udziału w innej czynności urzędowej. Zdaniem projektodawcy wskazanie minimalnej wysokości grzywny na kwotę 500 zł oraz maksymalnej na kwotę 5000 zł uzasadnione jest wagą spraw związanych z naruszeniem przepisów o ochronie danych osobowych, co wymaga zapewnienia sprawności i skuteczności postępowań w tych sprawach. Należy wskazać, że zgodnie z art. 189b k.p.a. przez administracyjną karę pieniężną rozumie się określoną w ustawie sankcję o charakterze pieniężnym, nakładaną przez organ administracji publicznej, w drodze decyzji, w następstwie naruszenia prawa polegającego na niedopełnieniu obowiązku albo naruszeniu zakazu ciążącego na osobie fizycznej, osobie prawnej albo jednostce organizacyjnej nieposiadającej osobowości prawnej. Zgodnie zaś z przepisem art. 189a § 1 k.p.a. w sprawach nakładania lub wymierzania administracyjnej kary pieniężnej lub udzielania ulg w jej wykonaniu stosuje się przepisy działu IVA Administracyjne kary pieniężne. Reasumując, w przypadku grzywien przewidzianych w k.p.a. (art. 88 oraz art. 96) z uwagi na fakt, iż grzywna ww. jest nakładana w drodze postanowienia, nie znajduje zastosowania dział IVA k.p.a. Jednakże, mając na uwadze obowiązujące w demokratycznym państwie prawnym zasady, w szczególności zasadę proporcjonalności oraz zasadę zaufania do organów państwa, w orzecznictwie i doktrynie postuluje się, aby wprowadzać gwarancje procesowe oraz przesłanki wymiaru sankcji administracyjnej w każdym przypadku wymierzania sankcji pieniężnych. Z uwagi na dużą rozpiętość przewidzianej sankcji pieniężnej (w przeciwieństwie do art. 88 k.p.a., gdzie maksymalna wysokość grzywny wynosi 200 zł) w ocenie projektodawcy, zasadne jest wprowadzenie przesłanek wymiaru kary grzywny.

Przepisy projektu mają na celu zapewnienie Prezesowi Urzędu narzędzia do natychmiastowej interwencji w sytuacji, gdy zostanie uprawdopodobnione, że dalsze przetwarzanie danych osobowych może spowodować poważne i trudne do usunięcia skutki. W takiej sytuacji Prezes Urzędu, w celu zapobieżenia tym skutkom, może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych, wskazując dopuszczalny zakres tego przetwarzania. Zdecydowano się wprowadzić do przepisów projektu ustawy instytucję skargi na to postanowienie. Należy wskazać, że wprowadzone przez projektodawcę uprawnienie jest uprawnieniem wykraczającym poza przewidziane w art. 58 rozporządzenia 2016/679. Państwa członkowskie uprawnione są do wprowadzania rozwiązań proceduralnych wykraczających poza przewidziane w rozporządzeniu 2016/679, o ile są one konieczne do zapewnienia jego skutecznego stosowania bądź w żadnym zakresie nie ograniczają pozycji

ustrojowej oraz zadań Prezesa Urzędu zagwarantowanych mu przepisami rozporządzenia 2016/679. Przyznanie Prezesowi Urzędu odrębnego środka prawnego do wydawania postanowień nakazujących czasowe ograniczenie przetwarzania danych w ocenie projektodawcy wzmacnia uprawnienia Prezesa Urzędu, a jego wprowadzenie możliwe jest w świetle przysługującej wszystkim państwom członkowskim autonomii proceduralnej. Wprowadzenie tak szczegółowej regulacji wskazującej wymogi, które muszą być spełnione, by postanowienie takie wydać, uzasadnione jest z kolei charakterem takich postanowień, które mogą mieć ogromny wpływ na działalność gospodarczą. Rozwiązanie wprowadzone do projektu ustawy o ochronie danych osobowych nie jest jednak rozwiązaniem obcym polskiemu porządkowi prawnemu. Z podobnymi rozwiązaniami mamy do czynienia chociażby w przypadku zabezpieczenia roszczeń w postępowaniu cywilnym bądź postępowaniu antymonopolowym w przypadku decyzji Prezesa UOKiK zobowiązującej przedsiębiorcę, któremu jest zarzucane stosowanie praktyk monopolowych, by w drodze decyzji zobowiązać go do zaniechania określonych działań. Skoro praktyki, które nie skutkują bezpośrednio naruszeniem praw podstawowych obywateli, zostały poddane takiej instytucji ochronnej, dziwi zamieszanie związane z ich wprowadzeniem w projekcie ustawy o ochronie danych osobowych. Wreszcie, jak zostało to już wskazane, zastosowanie przez Prezesa Urzędu takich środków tymczasowych obwarowane jest w projekcie restrykcyjnymi wymogami. Musi dojść do uprawdopodobnienia naruszenia, naruszenie powinno powodować poważne i trudne do usunięcia skutki, środek powinien przewidywać dopuszczalny zakres przetwarzania i czas jego obowiązywania. Zastosowanie tych środków następować powinno więc bez wątpienia wyjątkowo. Prezes Urzędu powinien wskazać również ograniczony zakres przetwarzania danych, nie powinien on jednak rodzić nieodwracalnych skutków jak np. usunięcie przetwarzania danych osobowych.

W projekcie ustawy – w zakresie rozstrzygnięć, jakie mogą zapaść po przeprowadzeniu postępowania, nie odesłano do art. 58 ust. 2 lit. b-j Rozporządzenia. Uznano za niecelowe przepisywanie oraz powoływanie się na obowiązujące przepisy Rozporządzenia w tym zakresie, wywołujące przecież bezpośredni skutek i podlegające bezpośredniemu zastosowaniu. Nowym elementem, a jednocześnie modyfikacją przepisów K.p.a., jest przepis art. 55 ust. 2 projektowanej ustawy, który nakłada na organ obowiązek poszerzenia uzasadnienia decyzji nakładającej na stronę administracyjną karę pieniężną o wskazanie przesłanek z art. 83 ust. 2 Rozporządzenia. Powyższe ma na celu ułatwienie sądowi oceny legalności samego nałożenia na stronę administracyjnej kary pieniężnej, jak i jej wysokości.

Zgodnie z projektowanymi przepisami, organy lub podmioty publiczne, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62), w stosunku do których Prezes Urzędu wydał prawomocną decyzję stwierdzającą naruszenie, niezwłocznie podają do publicznej wiadomości na swojej stronie internetowej lub stronie podmiotowej Biuletynu Informacji Publicznej informację o działaniach podjętych w celu wykonania decyzji. Celem tej regulacji jest przedstawienie opinii publicznej informacji o ewentualnych naruszeniach przepisów z zakresu ochrony danych osobowych przez podmioty publiczne oraz działaniach podjętych przez nie w celu usunięcia tych naruszeń. Natomiast w przepisach projektu ograniczono wysokość administracyjnej kary pieniężnej, którą można nałożyć na podmioty publiczne, do 100 000 zł. Projektodawca dostrzega bowiem specyfikę sektora publicznego, który powinien zapewniać pełną transparentność swoich działań. Zapewniając pełną transparentność działań Prezesa Urzędu, projektodawca nałożył na organ obowiązek każdorazowej oceny, czy wydawane przez niego decyzje nie powinny w interesie publicznym zostać przez niego udostępnione. Projektodawca odstąpił jednak od nałożenia na Prezesa Urzędu obowiązku publikowania przez niego wszystkich decyzji, kierując się chęcią zapewnienia sprawności działania organu i odciążając go od nadmiernych obowiązków administracyjnych. W przypadku niektórych z wydawanych decyzji, z uwagi na ich drobny przedmiot, ich udostępnienie może okazać się niecelowe.

Odnosząc się do projektu, wskazać należy, że projektodawca odstąpił od przesądzania, że każda z decyzji wydanych przez Prezesa Urzędu podlega rygorowi natychmiastowej wykonalności. Projektodawca uznał bowiem, że norma taka miałaby charakter informacyjny, a rygor natychmiastowej wykonalności decyzji Prezesa Urzędu będzie wynikał z właściwych przepisów powszechnie obowiązującego prawa - co nie wymaga powtarzania w projektowanej ustawie. Należy wyjaśnić, że zgodnie z projektem ustawy postępowanie przed Prezesem Urzędu jest postępowaniem jednoinstancyjnym, a więc od decyzji wydanej przez Prezesa Urzędu nie służy odwołanie (wniosek o ponowne rozpatrzenie sprawy). Konsekwencją wprowadzenia jednoinstancyjnego postępowania jest to, że decyzje wydane przez Prezesa Urzędu są ostateczne i wykonalne z mocy samego prawa. Podlegają one wykonaniu z chwilą doręczenia decyzji stronie. Rygor natychmiastowej wykonalności, zgodnie z art. 108 k.p.a., może zostać nadany decyzji nieostatecznej, a więc takiej, od której służy odwołanie, w administracyjnym toku instancji, *ergo* decyzji, od której nie służy odwołanie, nie nadaje się rygoru natychmiastowej wykonalności, ponieważ te decyzje są

ostateczne i podlegają natychmiastowemu wykonaniu z chwilą doręczania ich stronie. Usunięcie przez projektodawcę normy wprost przesądzającej o natychmiastowej wykonalności decyzji nie zmieni faktu, iż decyzje wydane przez Prezesa Urzędu w postępowaniu jednoinstancyjnym będą podlegały wykonaniu. Projektodawca, mając natomiast na uwadze, że zgodnie z Rozporządzeniem kary pieniężne mogą być bardzo dotkliwe dla ukaranych podmiotów, chciał wprowadzić wyjątek od wskazanej powyżej zasady, polegający na tym, że w przypadku wniesienia przez stronę skargi do sądu administracyjnego decyzja w zakresie dotyczącym administracyjnej kary pieniężnej podlega wstrzymaniu wykonania. Warto również zauważyć, że bez projektowanego przepisu strona mogłaby w skardze na decyzję Prezesa Urzędu wystąpić z wnioskiem o wstrzymanie wykonania decyzji w całości lub w części (art. 61 § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2017 r. poz. 1369, 1370 i 2451), zwanej dalej „p.p.s.a."), postanowiono jednak wprowadzić wstrzymanie wykonania decyzji w zakresie, w którym decyzja dotyczy administracyjnej kary pieniężnej z mocy ustawy bez konieczności składania przez stronę wniosku w tej sprawie. Strona na podstawie rzeczonego artykułu będzie mogła wystąpić z wnioskiem o wstrzymanie wykonania decyzji w pozostałym zakresie.

W projekcie uregulowano w zakresie niezbędnym postępowanie konsultacyjne, o którym mowa w art. 36 Rozporządzenia. Ograniczono się do wskazania wymogów formalnych pisma, ze względu na ekonomikę legislacyjną, poprzez odpowiednie odesłanie do art. 63 k.p.a. Ma to na celu możliwość weryfikacji wniosku poprzez obowiązek opatrzenia wniosku podpisem, gdyż obowiązek ten nie wynika bezpośrednio z art. 36 Rozporządzenia. Należy jednocześnie podkreślić, że do przeprowadzenia konsultacji nie znajdą zastosowania przepisy k.p.a., gdyż nieprzeprowadzenie konsultacji nie kończy się decyzją administracyjną ani żadnym innym władczym działaniem organu.

Projekt ma na celu dostosowanie polskiego prawa do wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie Wyrok Trybunału Sprawiedliwości UE w sprawie Maxa Schremsa, stwierdzający nieważność decyzji Komisji Europejskiej zatwierdzającej porozumienie Safe Harbor wyrok (C-362/14). W przedmiotowej sprawie TSUE stwierdził, że Komisja Europejska, która stwierdza, że państwo trzecie zapewnia odpowiedni stopień ochrony, nie stoi na przeszkodzie temu, aby organ nadzorczy państwa członkowskiego rozpatrzył skargę danej osoby związaną z ochroną jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, przekazanych z państwa członkowskiego

do tego państwa trzeciego, gdy osoba ta podnosi, że prawo i praktyka obowiązujące w tym państwie trzecim nie zapewniają odpowiedniego stopnia ochrony. Jednocześnie jednak TSUE wskazał jednoznacznie, iż tylko jemu przysługuje prawo do stwierdzenia nieważności takiej decyzji.

W efekcie powstała sytuacja, w której krajowy organ nadzorczy ma kompetencje do rozpatrywania spraw obywateli, których dane są przetwarzane na podstawie decyzji Komisji Europejskiej, lecz dopóki jest ona w porządku prawnym, dopóty *de facto* nie może on realizować w pełni swojej kompetencji. TSUE stwierdził także, że o ile sądy krajowe mają prawo badać ważność aktu unijnego, takiego jak decyzja Komisji, to jednak nie są one właściwe do samodzielnego stwierdzenia nieważności takiego aktu. *A fortiori*, krajowe organy nadzorcze nie mają prawa samodzielnie stwierdzić nieważności takiej decyzji przy rozpatrywaniu, dotyczącej zgodności decyzji Komisji Europejskiej. Także krajowe sądy taką kompetencją nie dysponują.

W konkluzji TSUE wskazał, że jeżeli organ nadzorczy uzna zarzuty podniesione przez osobę, która wniosła do niego skargę dotyczącą ochrony jej praw i wolności w zakresie przetwarzania danych osobowych, za zasadne, organ ten powinien – mieć prawo pozywania do sądu. W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji.

Mając na uwadze podstawową zasadę ustrojową, iż kontrola administracji publicznej jest dokonywana przez sądy administracyjne, projektodawca zdecydował się pozostawić ww. kompetencję sądom administracyjnym. Należy jednak wskazać, że podstawową zasadą działania sądów administracyjnych jest zasada skargowości, czyli badania wydanych przez organy administracji publicznej aktów administracyjnych, które są zaskarżane przez strony postępowania. Ta podstawowa funkcja i model kontroli sądowoadministracyjnej wynikającej z art. 1 i art. 2 p.p.s.a. nie znajduje zastosowania ww. przypadku.

W efekcie projektodawca zdecydował się wprowadzić odrębną procedurę w ustawie o ochronie danych osobowych. Nie jest to jednak procedura oderwana w całości od rozwiązań przewidzianych w k.p.a. oraz p.p.s.a. Zgodnie z art. 1 p.p.s.a., ustawa ta normuje postępowanie sądowe w sprawach z zakresu kontroli działalności administracji publicznej

oraz w innych sprawach, do których jego przepisy stosuje się z mocy ustaw szczególnych (sprawy sądowoadministracyjne). Prawo do wprowadzenia nowej kompetencji dla sądów administracyjnych, niezwiązanych wyłącznie z „kontrolą administracji publicznej", wynika wprost z art. 1 ww. ustawy. Zgodnie natomiast z art. 63 i art. 64 p.p.s.a., jeżeli ustawy tak stanowią, postępowanie sądowe wszczyna się na wniosek. Wniosek składa się bezpośrednio do sądu. Wniosek powinien czynić zadość wymaganiom pisma w postępowaniu sądowym, a ponadto zawierać określenie żądania, jego podstawy i uzasadnienie oraz oznaczenie stron i organów, a także spełniać inne wymagania określone w przepisach szczególnych. Przepis ten stanowi także, że do wniosku stosuje się odpowiednio przepisy o skardze, jeżeli ustawa nie stanowi inaczej. W efekcie w ustawie o ochronie danych osobowych przyjęto następujące rozwiązanie.

Prezes Urzędu, podejmując z urzędu lub na wniosek postępowanie w sprawie stwierdzenia naruszenia przepisów o ochronie danych osobowych, ustalając, iż przetwarzanie danych osobowych strony postępowania następuje m.in. na podstawie decyzji Komisji Europejskiej, oraz uznając, iż istnieją uzasadnione wątpliwości, że decyzja Komisji Europejskiej jest niezgodna z prawem Unii Europejskiej, na podstawie art. 97 k.p.a. zawiesza swoje postępowanie. Zgodnie bowiem z art. 97 § pkt 4 k.p.a. organ zawiesza postępowanie, gdy rozpatrzenie sprawy i wydanie decyzji zależy od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd. Jak wskazuje się w literaturze, przepis art. 97 § 1 pkt 4 k.p.a. nie daje podstaw do tego, aby zawęzić krąg podmiotów kompetentnych do rozstrzygnięcia zagadnienia wstępnego tylko do polskich sądów lub organów. Przemawia bowiem przeciwko temu zarówno wykładnia językowa, jak i systemowa, odwołująca się do koncepcji źródeł prawa powszechnie obowiązującego (W. Chróścielewski). Ponadto, jak wskazał WSA w Warszawie SA/Wa 1898/06, Legalis, pojęcie sądu, użyte w art. 97 § 1 pkt 4 k.p.a., musi podlegać wykładni dynamicznej i celowościowej, uwzględniającej zmiany systemu wymiaru sprawiedliwości (powołanie TK) oraz dopuszczenie jurysdykcji sądów międzynarodowych, takich jak Europejski Trybunał Praw Człowieka oraz Trybunał Sprawiedliwości UE. W niniejszej sytuacji za powyższym w ocenie projektodawcy przemawia fakt, iż sprawa przed TSUE w sprawie ważności decyzji administracyjnej zostanie wszczęta w indywidualnym postępowaniu. Następnie Prezes Urzędu wystąpi na podstawie przepisów ustawy o ochronie danych osobowych do sądu administracyjnego z wnioskiem (będzie to wniosek, o którym mowa w art. 63-64 p.p.s.a.) o wydanie orzeczenia w sprawie ważności decyzji Komisji Europejskiej. W celu wyjaśnienia należy wskazać, że zgodnie z

ogólną regułą zawartą w art. 13 p.p.s.a. sądem właściwym do rozpatrzenia wniosku Prezesa Urzędu będzie wojewódzki sąd administracyjny.

Następnie, z uwagi na wyłączną kompetencję TSUE w zakresie stwierdzenia ważności decyzji Komisji Europejskiej, sąd administracyjny będzie, w przypadku przyjęcia wątpliwości Prezesa Urzędu za zasadne, występował z zapytaniem prawnym do TSUE. W przeciwnym wypadku sąd administracyjny wyda stosowne postanowienie.

Obowiązek wystąpienia przez sąd administracyjny z pytaniem prawnym do TSUE w ocenie projektodawcy będzie wynikał z faktu, iż postępowanie przez sądem administracyjnym będzie miało charakter jednoinstancyjny. Od postanowienia sądu administracyjnego nie będzie przysługiwał środek odwoławczy. Zgodnie natomiast z art. 267 Traktatu o funkcjonowaniu Unii Europejskiej (2016/C 202/01), Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania w trybie prejudycjalnym o wykładni Traktatów oraz o ważności i wykładni aktów przyjętych przez instytucje, organy lub jednostki organizacyjne Unii. W przypadku gdy pytanie z tym związane jest podniesione przed sądem jednego z państw członkowskich, sąd ten może, jeśli uzna, że decyzja w tej kwestii jest niezbędna do wydania wyroku, zwrócić się do Trybunału z wnioskiem o rozpatrzenie tego pytania. W przypadku gdy takie pytanie jest podniesione w sprawie zawisłej przed sądem krajowym, którego orzeczenia nie podlegają zaskarżeniu według prawa wewnętrznego, sąd ten jest zobowiązany wnieść sprawę do Trybunału.

Celem wyjaśnienia wszelkich wątpliwości należy wskazać, że na podstawie projektowanej regulacji sądowi administracyjnemu nie będzie przysługiwało uprawnienie do stwierdzenia nieważności powołanych w przepisie decyzji Komisji Europejskiej. Tego rodzaju regulacja naruszałaby niezależność sądu administracyjnego, narzucając obligatoryjne działanie procesowe. Dodatkowo zgodnie z utrwalonym orzecznictwem TSUE, sąd krajowy państwa członkowskiego nie ma kompetencji orzekania o ważności aktów prawa UE.

Projektodawca zdecydował się również ograniczyć zastosowanie wskazanych powyżej regulacji wyłącznie do decyzji Komisji Europejskiej, które dotyczą przekazywania danych osobowych do państw trzecich oraz organizacji międzynarodowych, nie chcąc dokonywać rozszerzającej wykładni wyroku TSUE. Jak zostało to już bowiem wskazane, wprowadzenie do projektu przedmiotowej regulacji uzasadnione jest treścią wyroku TSUE w sprawie Maxa Schremsa, stwierdzającego nieważność decyzji Komisji Europejskiej zatwierdzającej porozumienie Safe Habor wyrok (C-362/14), a więc obejmującego swoim zakresem

przedmiotowym co do zasady sprawy dotyczące międzynarodowych transferów danych. Od strony formalnoprawnej, w projekcie zawarto przepisy, które mają na celu dostosowanie wymagań wniosku, który będzie składał Prezes Urzędu do sądu administracyjnego, do wymagań określonych do złożenia pytania prejudycjalnego, o którym mowa w art. 267 Traktatu o funkcjonowaniu Unii Europejskiej. Zmiany te mają także na celu przyśpieszenie postępowania w sprawie rozpoznania wniosku prowadzonego przed sądem administracyjnym. Treść przepisu określającego wymogi dla wniosku Prezesa Urzędu (art. 71 ust. 2) została opracowana w oparciu o dokument pn. „Zalecenia dla sądów krajowych dotyczące składania wniosków o wydanie orzeczenia w trybie prejudycjalnym (2016/C 439/01)", który został opublikowany w Dzienniku Urzędowym Unii Europejskiej z 25.11.2016 nr C 439/1. W przepisie zaproponowano także, że stroną w postępowaniu przed sądem administracyjnym będzie wyłącznie Prezes Urzędu. W celu zagwarantowania stronom prawa przedstawienia stanowiska w sprawie zawarto przepis, zgodnie z którym wniosek Prezesa Urzędu winien zawierać m.in. „stanowisko strony podniesione w postępowaniu przed organem, jeżeli zostało przedstawione przez stronę". W celu zwiększenia pluralizmu, zdecydowano się wprowadzić regulację, zgodnie z którą wniosek podlega rozpatrzeniu na posiedzeniu niejawnym w składzie 3 sędziów. Powyższe stanowi wyjątek od ogólnej zasady rozpatrywania sprawy w ww. formule w składzie wyłącznie 1 sędziego. Dodatkowo należy wskazać, iż o ile od rozpoznania przez sąd administracyjny wniosku o charakterze merytorycznym, tj. oceny argumentów i okoliczności podniesionych przez Prezesa Urzędu, nie będzie przysługiwał środek odwoławczy, o tyle ocena wymogów formalnych wniosku wynikających m.in. z art. 64 p.p.s.a. w zw. art. 71 projektu ustawy będzie odbywała się na zasadach ogólnych ustawy - Prawo o postępowaniu przed sądami administracyjnymi. Dotyczy to w szczególności instytucji wezwania do uzupełnienia wniosku oraz przepisów dotyczących środków odwoławczych np. na postanowienie sądu administracyjnego o odrzuceniu wniosku z uwagi na niespełnienie wymogów formalnych. W celu przyśpieszenia postępowania w sprawie rozpatrzenia wniosku oraz dalszych prac (przy uznaniu przez sąd administracyjny zadania pytania do TSUE za zasadne) wprowadzono obowiązek doręczenia wraz z wnioskiem treści wniosku w postaci elektronicznej w wersji pozwalającej na jej edycję. Jest to pomocnicza forma dla wniosku papierowego ułatwiająca sądowi administracyjnemu skonstruowanie pytania prawnego zgodnie z wymaganiami określonymi w „Zaleceniach dla sądów krajowych dotyczących składania wniosków o wydanie orzeczenia w trybie prejudycjalnym (2016/C 439/01)". Zalecenia zawierają także wymagania o charakterze redakcyjno-technicznym, a posiadanie przez sąd elektronicznej i edytowalnej kopii wniosku przyśpieszy

sporządzenie docelowego pytania i jego rozpatrywanie przez TSUE. Projektowane przepisy były przedmiotem konsultacji z Naczelnym Sądem Administracyjnym.

Rozdział 8. Europejska współpraca administracyjna. Przepisy ustawy mają zapewnić skuteczne stosowanie rozdziału VII Rozporządzenia regulującego zagadnienia europejskiej współpracy administracyjnej w sprawach ochrony danych osobowych. Mimo że przepisy proceduralne wprowadzone do rozdziału VII Rozporządzenia są bezpośrednio skuteczne i co do zasady w sposób wyczerpujący regulują zasady prowadzenia współpracy, bez podjęcia krajowej uzupełniającej aktywności ustawodawczej ich zastosowanie byłoby w polskim porządku prawnym w niektórych obszarach niemożliwe.

Koniecznym było doprecyzowanie formy prawnej działań podejmowanych przez Prezesa Urzędu na podstawie art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 Rozporządzenia. Wszystkie z powołanych przepisów zobowiązują Prezesa Urzędu do wydawania środków tymczasowych, którym w polskim porządku prawnym nadana została forma postanowienia. Zgodnie z motywem 137 Rozporządzenia, organ nadzorczy powinien w razie pilnej potrzeby podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, mieć możliwość przyjmowania na swoim terytorium należycie uzasadnionych środków tymczasowych o określonym czasie obowiązywania. Motyw znajduje swoje odzwierciedlenie w powołanych już art. 61 ust. 8, art. 62 ust. 7 oraz art. 66 ust. 1 Rozporządzenia. Nie jest więc możliwe zapewnienie przez ustawodawcę krajowego skutecznego stosowania tych przepisów Rozporządzenia, bez przyznania Prezesowi Urzędu uprawnienia do wydawania takich środków tymczasowych.

W Rozporządzeniu brak jest jakichkolwiek regulacji prawnych w zakresie języka prowadzenia współpracy w sprawach ochrony danych osobowych. Należy więc przyjąć, że wszelkie informacje pomiędzy organem a Komisją Europejską, Europejską Radą Ochrony Danych oraz organami nadzorczymi mogą być przesyłane w każdym z oficjalnych języków UE. Powyższe stanowi jednak dodatkowy czynnik znacznie utrudniający współpracę w ramach mechanizmu zgodności. O ile bowiem, w ramach aparatu administracyjnego Komisji Europejskiej zatrudnieni są urzędnicy, władający biegle wszystkimi językami UE, o tyle organy nadzorcze państw członkowskich pracownikami takimi nie dysponują. Art. 6 rozporządzenia Rady nr 1/58 z 15 kwietnia 1958 r. poświęconego językom UE, zwanego „Kartą Języków Unii Europejskiej", przyznaje instytucjom unijnym możliwość wyboru języka, w którym rozpatrywane były określone kategorie spraw. Działanie takie mogłoby zostać jednak uznane za sprzeczne z jednym z zadań, przed jakim stoi Komisja, tj.

odpowiedzialność, za upowszechnianie wiedzy na temat wielojęzyczności i opiekę nad nią - powołana została zresztą w tym celu instytucja Komisarza ds. Wielojęzyczności. W związku z powyższym ustawodawca unijny odstąpił od regulowania jakichkolwiek zagadnień związanych z językiem prowadzonej współpracy. Uwzględniając powyższe oraz jedną z podstawowych wartości, jaką jest wielokulturowość UE, przepisy ustawy nakładają obowiązek kierowania korespondencji przez Prezesa Urzędu w jednym z języków urzędowych państwa członkowskiego będącego adresatem danej czynności lub w języku angielskim.

Dokonywanie efektywnej współpracy wymaga dokładnego doprecyzowania zakresu zadań podejmowanych przez każdy z organów nadzorczych państw członkowskich.

Rozdział 9. Kontrola przestrzegania przepisów o ochronie danych osobowych. W przepisach rozdziału 9 uregulowano postępowanie kontrolne. Przepisy tego rozdziału będą miały zastosowanie w przypadku czynności kontrolnych prowadzonych w ramach postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, w przypadku kontroli planowych, jak również kontroli doraźnych. Kontrole będą przeprowadzane przez upoważnionych pracowników Urzędu Ochrony Danych Osobowych. W ocenie projektodawcy, celem wyeliminowania ryzyka jakichkolwiek nieprawidłowości w zakresie przeprowadzanych kontroli, wzór legitymacji służbowej okazywanej w trakcie przeprowadzanej kontroli powinien zostać określony w drodze rozporządzenia. Projektodawca nie zdecydował się skorzystać z uprawnienia z art. 62 ust. 3 Rozporządzenia i przyznać tym osobom uprawnienie do wykonywania ich własnych uprawnień w zakresie postępowania wyjaśniającego. Osoby te będą wykonywały uprawnienia takie jak przysługują pracownikom Urzędu Ochrony Danych Osobowych. Zakres udzielanych upoważnień do przeprowadzenia kontroli określają przepisy projektu. Dla zapewnienia możliwości przeprowadzenia kontroli pod nieobecność kontrolowanego przewidziano, że upoważnienie do przeprowadzenia kontroli będzie mogło być okazane pracownikowi kontrolowanego lub przywołanemu świadkowi, którym powinien być funkcjonariusz publiczny. W związku ze stałym rozwojem nowych technologii oraz założeniami, na jakich opiera się Rozporządzenie, ochrona danych osobowych wymaga wiedzy z pogranicza prawa, sektora IT oraz analityki. Projektodawca dostrzega więc potrzebę skorzystania przez Prezesa Urzędu z zaplecza eksperckiego, przewidując możliwość upoważnienia przez niego do udziału w kontroli osoby posiadającej taką wiedzę. Zakres uprawnień kontrolujących oraz obowiązków kontrolowanych określa projekt. Projektodawca zdecydował się wprowadzić ograniczenie

czasu przeprowadzania kontroli do godzin 6.00 – 22.00, uznając, iż ochrona danych osobowych nie będzie wymagała podjęcia aż tak nagłych czynności kontrolnych. Postanowiono zatem wyłączać z mocy ustawy możliwość przeprowadzenia kontroli poza ww. godzinami. Ważną i nową regulacją, mającą na celu skuteczne przeprowadzenie czynności kontrolnych, są przepisy pozwalające kontrolującym korzystać z pomocy funkcjonariuszy innych organów kontroli lub Policji. W szczególności należy wskazać, że Policja zobowiązana będzie do udzielenia pomocy nie tylko w przypadkach, o których mowa w art. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067), ale również, gdy jest to konieczne, gdy kontrolujący natrafi na opór, który utrudnia lub uniemożliwia mu wykonywanie kontroli, albo jeżeli istnieje uzasadnione przypuszczenie, że na taki opór natrafi. Uwzględniając dotychczasową praktykę działania GIODO, sytuacje takie występują rzadko, ale ich wystąpienie uniemożliwia skuteczne przeprowadzenie kontroli. Zgodnie z przepisami projektu kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Rozdział 10. Odpowiedzialność cywilna i postępowanie przed sądem. Rozdział 10 projektu ustawy odnosi się do odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych. Projekt wdraża do polskiego porządku prawnego regulację art. 79 ust. 1 Rozporządzenia. Zgodnie z treścią tego przepisu: „1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia.". Art. 79 ust. 1 Rozporządzenia wymaga od państw członkowskich, aby w ich systemach prawnych istniały skuteczne środki ochrony prawnej przed sądem, w przypadku gdy podmiot danych uzna, że prawa przysługujące mu na mocy Rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia. Art. 79 ust. 1 Rozporządzenia dotyczy zarówno środków o charakterze materialnoprawnym, jak i procesowym. Art. 79 ust. 1 Rozporządzenia nie wymaga wprowadzenia do systemu prawa państwa członkowskiego nowego środka na płaszczyźnie prawa materialnego, jeżeli obowiązujące przepisy mogą stanowić skuteczną podstawę roszczeń związanych z naruszeniem ogólnego rozporządzenia (czy ogólnie przepisów o ochronie danych

osobowych). W tym miejscu należy zwrócić uwagę, iż realizacja normy kompetencyjnej wskazanej w art. 79 ust. 1 Rozporządzenia nie może naruszać bezpośrednio skutecznej normy wyrażonej w art. 82 Rozporządzenia (tj. nie może ograniczać dochodzenia roszczeń w oparciu o tę podstawę prawną). Zgodnie z treścią art. 82 ust. 1 Rozporządzenia każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego Rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. W art. 82 ust. 1 Rozporządzenia chodzi więc o roszczenia majątkowe (art. 82 ust. 5 Rozporządzenia mówi o „zapłacie" odszkodowania), które można dochodzić w razie zaistnienia szkody majątkowej lub niemajątkowej (zob. M. Gumularz, Wpływ regulacji 37 odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich, Europejski Przegląd Sądowy z 2017, nr 5). W związku z powyższym projektowane regulacje dotyczą roszczeń odszkodowawczych, które mogą być realizowane w przypadku poniesienia szkody majątkowej lub niemajątkowej w wyniku naruszenia przepisów Rozporządzenia w oparciu o art. 82 Rozporządzenia. Projektowane przepisy mają charakter porządkowy i przesądzają cywilnoprawny tryb dochodzenia roszczeń wskazanych w projekcie. W związku z tym sądy okręgowe będą właściwe w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, niezależnie od tego, czy chodzić będzie o roszczenia majątkowe (niezależnie od wartości przedmiotu sporu) czy niemajątkowe. Decyzja o przyznaniu sądom okręgowym właściwości w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych podyktowana została względami ekonomiki w tym chęcią zapewnienia szybkości postępowania. Liczba spraw rozpatrywanych przez sądy okręgowe jest mniejsza niż sądy rejonowe. Przepis ten stanowi regulację szczególną względem art. 17 pkt 4 Kodeksu postępowania cywilnego. Celem wprowadzenia przedmiotowych regulacji do projektu jest udrożnienie i przyspieszenie komunikacji pomiędzy sądami powszechnymi a Prezesem Urzędu. Należy zwrócić uwagę, iż wniesienie pozwu w sprawach, o których mowa w projekcie, obliguje sąd – przed którym toczy się postępowanie - do zawiadomienia Prezesa Urzędu. W ocenie projektodawcy ważnym do wskazania jest również, że wprowadzenie do projektu wskazanych regulacji nie ma wpływu na toczące się obecnie postępowania. W projekcie uregulowano wzajemną relację pomiędzy toczącymi się postępowaniami sądowoadministracyjnymi oraz cywilnymi. Zgodnie z propozycją sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed Prezesem Urzędu. Sąd umarza natomiast postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu

lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a p.p.s.a., uwzględnia roszczenie dochodzone przed sądem.

Wskazano także w projekcie ustawy, że ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 p.p.s.a., wiążą sąd w postępowaniu o naprawnienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów.

Dodatkowo w projekcie wskazano, że w sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie w postępowaniu przed sądem, Prezes Urzędu może wytaczać powództwa na rzecz osoby, której dane dotyczą, za jej zgodą, a także wstępować, za zgodą powoda, do postępowania w każdym jego stadium. W pozostałych sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych Prezes Urzędu może wstępować, za zgodą powoda, do postępowania przed sądem w każdym jego stadium, chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych.

Rozdział 11. Przepisy o administracyjnych karach pieniężnych i przepisy karne. Przepisy rozdziału 11 projektu dotyczą administracyjnych kar pieniężnych oraz zasad odpowiedzialności karnej. W pierwszej kolejności należy wskazać, iż przesłanki ich nakładania i maksymalne wysokości wynikają wprost z Rozporządzenia (art. 83 ust. 1–6). Odnosząc się do katalogu podmiotów, na które takie kary mogą być nakładane, prawodawca unijny wprowadził możliwość szczególnego uregulowania przez państwa członkowskie kwestii nakładania tych kar na organy i podmioty publiczne (art. 83 ust. 7). Zgodnie bowiem z tym przepisem każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

Polski prawodawca skorzystał z możliwości, jaką daje art. 83 ust. 7 Rozporządzenia, i postanowił, że kary mogą być nakładane jedynie na podmioty wymienione w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, Narodowy Bank Polski oraz instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych i wysokość kar nie może przekroczyć 100 000 zł. Narodowy Bank Polski jest organem przewidzianym w Konstytucji Rzeczypospolitej Polskiej i bez wątpienia jest organem publicznym. Jednocześnie jednak nie znajduje się on w katalogu podmiotów, o

których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, co wymusiło na projektodawcy jego enumeratywne wskazanie w projektowanym przepisie.

Przede wszystkim trzeba zauważyć, że podmioty publiczne są finansowane ze środków budżetu państwa, a środki z administracyjnych kar pieniężnych stanowią dochód budżetu państwa. A zatem w przypadku nałożenia na podmiot publiczny administracyjnej kary pieniężnej środki z tej kary pośrednio trafiałyby z powrotem do tego podmiotu. O ile bowiem w odniesieniu do podmiotów spoza administracji publicznej administracyjna kara pieniężna jest dotkliwą sankcją, to nie można zgodzić się, iż taki sam skutek odnosiła ona będzie w stosunku do podmiotów publicznych. Zatem kara ta nie spełniałaby swego represyjnego celu. Dodatkowo nakładanie kar na administrację publiczną w znacznych ilościach pośrednio obciąża obywateli, uwzględniając, że środki publiczne pochodzą również z obciążeń podatkowych wnoszonych przez obywateli.

Projektodawca zdecydował się również wprowadzić wyjątek w zakresie nakładania administracyjnych kar finansowych, ograniczając maksymalny wymiar kary wymierzanej wobec instytucji kultury do 10 000 zł. Warto przy tym pamiętać, że Konstytucja Rzeczypospolitej Polskiej wprowadza dwie ważne zasady działania państwa w tej dziedzinie:

- zasadę upowszechniania dóbr kultury, mającą istotne znaczenie dla poznawania kultury, uczestniczenia w niej, tworzenia wspólnoty narodowej oraz procesu patriotycznego wychowania i kształtowania postaw obywatelskich,

- zasadę zapewnienia równego dostępu do tych dóbr, które stanowią źródło tożsamości Narodu, jego trwania i rozwoju.

Realizacja ww. zasad następuje w formie działań niewładczych, nie może wręcz ze względu na swój charakter być zabezpieczona przymusem administracyjnym. Uczestniczenie w kulturze jako jej odbiorca, animator czy twórca, tj. kreowanie usług kulturalnych czy korzystanie z usług kulturalnych, jak i z mecenatu państwa, ma charakter dobrowolny i niekiedy wiąże się z koniecznością umożliwienia przetwarzania danych osób korzystających z ofert największego mecenasa kultury, jakim jest państwo i jego instytucje. Muzea, teatry i podobne instytucje zwykle przetwarzają podstawowe dane osobowe, takie jak: imię, nazwisko, adres i dane kontaktowe. Dane te są potrzebne najczęściej w związku z korzystaniem z karnetów, newsletterów itp. usług. Dane tego rodzaju są zresztą coraz częściej ogólnodostępne w sieci i służą zapewnieniu dostępu do oferty kulturalnej, zachęceniu do korzystania z niej, zaktywizowaniu i promowaniu działań animatorskich czy twórczych.

Zagrożenie wysokimi karami administracyjnymi w ocenie projektodawcy zniechęciłoby do prowadzenia tego typu działalności, a tym samym pozbawiłoby, a w każdym razie znacznie ograniczyło, obywatelom możliwość dostępu do kultury, w szczególności w wymiarze lokalnym. Tam, gdzie realne nakłady na kulturę są najniższe (gminy wiejskie czy małe miasta) i funkcjonują najbardziej podstawowe formy działalności kulturalnej (tj. biblioteka gminna i ośrodek kultury, a często wspólna biblioteka gminy i powiatu czy biblioteka i ośrodek połączone w jedną instytucję, tak aby jak najwięcej środków wydatkowanych było wyłącznie na samą działalność kulturalną, a nie jej obsługę czy administrowanie nią), trudno byłoby zaakceptować dodatkowe obciążenia finansowe, wynikające z kar stanowiących znaczący ułamek rocznego budżetu instytucji. Z kolei należy też wskazać, że co do zasady kultura jest traktowana, w wielu regulacjach ustrojowych, administracyjnych, karnych, cywilnoprawnych czy finansowo-podatkowych, w sposób szczególny, zwłaszcza w zestawieniu z innymi sferami działalności czy usług publicznych, i to tak w zakresie prawa unijnego, jak krajowego. Przykładowo, do działalności kulturalnej w pewnym zakresie nie stosuje się w ogóle ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U z 2017 r. poz. 1579) (art. 4d ust. 1 pkt 2 tej ustawy). Ponadto ogranicza się jawność informacji związanych z postępowaniem o udzielenie zamówienia dostaw lub usług z zakresu działalności kulturalnej (art. 8 ust.4 rzeczonej ustawy) czy wprowadza bardziej złagodzony reżim udzielania zamówień (taki jak do innych tzw. usług społecznych), który oddaje inicjatywę w zakresie kształtu postępowania zamawiającemu (art. 138p i nast. ustawy). Takie uproszczenia czy wyłączenia w ramach procedur przy udzielaniu zamówień na dostawy czy usługi z zakresu kultury mają swoje umocowanie w prawodawstwie unijnym – *vide* np. motyw 113, art. 4, art. 21 i art. 74 oraz załącznik XIV dyrektywy 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE, tzw. dyrektywy klasycznej, albo załącznik XVII dyrektywy 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającej dyrektywę 2004/17/WE z dnia 28 marca 2014 r., tzw. dyrektywy sektorowej. Kultura i dziedzictwo kulturowe są również szczególnie traktowane w przepisach o pomocy publicznej. Rozporządzenie Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1) nie wyłącza wprawdzie kultury spod reguł dotyczących pomocy publicznej, jednakże znacząco ogranicza ich stosowanie w tej dziedzinie. Przykładowo, pod pewnymi warunkami, pomoc na kulturę i zachowanie dziedzictwa kulturowego jest uznana za zgodną z rynkiem

wewnętrznym i wyłączona z obowiązku zgłoszenia. Dotyczy to m.in. pomocy udzielanej takim jednostkom jak „muzea, archiwa, biblioteki, ośrodki lub przestrzenie kulturalne i artystyczne, teatry, opery, sale koncertowe, inne organizacje, wystawiające widowiska sceniczne, instytucje odpowiedzialne za dziedzictwo filmowe oraz inne podobne infrastruktury, organizacje i instytucje kulturalne i artystyczne" (art. 53 ust. 2 pkt a). Niezależnie od regulacji szczegółowych warto przypomnieć, że artykuł 167 Traktatu o funkcjonowaniu Unii Europejskiej uznaje znaczenie, jakie dla Unii i państw członkowskich ma wspieranie kultury, oraz stanowi, że Unia powinna uwzględniać aspekty kulturalne w swoim działaniu, zwłaszcza w celu poszanowania i popierania różnorodności jej kultur. Również ostatnio Unia Europejska przystąpiła do prac nad zrewidowaniem stawek podatku od towarów i usług (dalej „VAT") na tzw. e-booki. Komisja Europejska przedstawiła pakiet rozwiązań „mających na celu poprawę warunków prowadzenia działalności przez przedsiębiorstwa zajmujące się handlem elektronicznym pod względem podatku VAT". Te działania także wskazują na znaczenie i szczególne podejście UE do spraw kultury. Komisja Europejska przedłoży wniosek dotyczący dyrektywy Rady zmieniającej dyrektywę 2006/112/WE w odniesieniu do stawek podatku od wartości dodanej stosowanego do książek, gazet i czasopism (projekt Komisji Europejskiej z 1 grudnia 2016 r., COM(2016) 758 final). Projekt ten zapowiedziany został w komunikacie Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego dotyczącym planu działania w sprawie VAT (zob. COM(2016) 148 final). W uzasadnieniu do wniosku Komisja wskazuje w szczególności, że „mimo że istnieją różnice między publikacjami drukowanymi i publikacjami elektronicznymi pod względem formatu, oba rodzaje publikacji oferują taką samą treść czytelniczą dla nabywców". Można zatem oczekiwać, że nowa koncepcja zmian dotyczących stawek VAT w sektorze handlu elektronicznego poskutkuje w efekcie zrównaniem stawek VAT na książki papierowe i ebooki. Z kolei polski ustawodawca w ramach ustawy o organizowaniu i prowadzeniu działalności kulturalnej gwarantuje instytucjom kultury - jak najdalej możliwą w sferze publicznej - samodzielność prawną, organizacyjną i finansową, przyznając im status osób prawnych (*vide* art. 14). Zabezpiecza obowiązek finansowania przez organizatorów (art. 12) oraz samodzielność w działaniu (art. 15-17 i art. 27), tak aby instytucje te mogły przede wszystkim realizować zadania związane z upowszechnianiem i ochroną kultury, wspieraniem i promowaniem twórczości, edukacją i oświatą kulturalną czy działaniami i inicjatywami kulturalnymi - w sposób jak najmniej obciążony typowymi dla administracji wymaganiami czy rygorami. W sferze podatkowej polski ustawodawca przewiduje natomiast specjalne rozwiązania promujące twórców i

artystów oraz wydatki na cele kulturalne, w tym darowizny. Analogicznie w systemie ubezpieczeń społecznych artyści i twórcy posiadają pewne preferencyjne rozwiązania emerytalne (*vide* art. 8 ust. 5 pkt 2, ust. 7 i 9, art. 36 ust. 4a, art. 47 ust. 1a ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2017 r. poz. 1778 oraz z 2018 r. poz. 106, 138, 357 i 398) oraz art. 6 ust. 2 pkt 9 lit. b ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych). Z powyższych powodów w ocenie projektodawcy za zasadne należy uznać szczególne potraktowanie działalności kulturalnej, w tym prowadzonej przez instytucje kultury, w przepisach o ochronie danych osobowych poprzez wyłączenie stosowania w stosunku do nich administracyjnych kar pieniężnych.

Zgodnie z projektem ustawy Prezes Urzędu Ochrony Danych Osobowych „może na wniosek podmiotu ukaranego odroczyć uiszczenie kary pieniężnej albo rozłożyć ją na raty ze względu na ważny interes wnioskodawcy". Na podstawie projektu ustala się odsetki w wysokości 50% stawki odsetek za zwłokę. Wprowadzona na podstawie ww. przepisu ulga może spełniać przesłanki pomocy publicznej określone w art. 107 ust. 1 TFUE, gdyż: może powodować uszczuplenie dochodów państwa, ma charakter selektywny (skierowana jest do określonych podmiotów), może stanowić dla zgłaszających korzyść, której nie uzyskaliby w normalnych warunkach rynkowych, a także - jako że wśród beneficjentów tej ulgi znajdują się przedsiębiorcy działający na rynkach otwartych na konkurencję - może zakłócić lub grozić zakłóceniem konkurencji i wpłynąć na wymianę handlową między państwami członkowskimi UE.

W zakresie przepisów karnych Generalnym celem projektodawcy było nierozbudowywanie przepisów karnych i ich ograniczenie do niezbędnych z punktu widzenia systemu ochrony danych osobowych. Wprowadzone do projektu regulacje nie są więc kopią obecnych rozwiązań. Obowiązujące dziś przepisy wskazują wiele czynów zabronionych, ale jednocześnie zbyt ogólnie opisują znamiona poszczególnych z nich. W konsekwencji prokuratorzy i sądy niechętnie sięgają do tych regulacji, co z kolei przekłada się na niewielką liczbę prowadzonych postępowań. Odpowiedzialność karna ma być jednak wyjątkiem przewidzianym wyłącznie dla najcięższych naruszeń przepisów. Będzie stanowiła uzupełnienie dla szeroko uregulowanej odpowiedzialności administracyjnej i cywilnej, a nie główną oś gwarancji przestrzegania przepisów, jak obecnie. Przyjęto więc, iż podstawowymi „sankcjami" za naruszenie przepisów o ochronie danych osobowych są nakładane na administratora lub podmiot przetwarzający obowiązki wynikające z prawa administracyjnego

oraz administracyjne kary pieniężne. Tym niemniej dla zapewnienia skuteczności systemu ochrony danych osobowych przewidziano sankcję karną za udaremnianie lub utrudnianie kontrolującemu prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych. Regulacja w tym zakresie obowiązuje również na gruncie obowiązującej Ustawy.

Orzekanie w tych sprawach następowało będzie na podstawie przepisów ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 2017 r. poz. 2204 oraz z 2018 r. poz. 20 i 305). Zgodnie z treścią projektowanych przepisów, kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, będzie podlegał grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Przepisy penalizują również przetwarzanie zwykłych i szczególnych kategorii danych (z art. 9 Rozporządzenia) bez podstawy prawnej. Mając na względzie dobro podmiotów danych oraz wagę naruszenia, jakim jest przetwarzanie danych osobowych, uznano, że przetwarzanie danych bez podstawy prawnej, a więc nieuprawnione i umyślne przetwarzanie, powinno być zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności. Projektodawca zdecydował się jedynie rozróżnić maksymalny wymiar możliwej kary od kategorii przetwarzanych danych, w ślad za intencją ustawodawcy unijnego, który wprowadza dwie kategorie danych: danych szczególnie chronionych oraz danych zwykłych. Jednocześnie projektodawca nie zdecydował się zmienić obowiązujących obecnie maksymalnych wymiarów kar, wskazując je na poziomie dwóch lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych zwykłych oraz trzech lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych wrażliwych. Należy jednocześnie zwrócić uwagę, iż naruszenie przepisów o ochronie danych może stanowić czyn realizujący znamiona określone w przepisach Kodeksu karnego np. w ramach rozdziału XXXIII Przestępstwa przeciwko ochronie informacji.

Rozdział 13. Przepisy zmieniające. Przepisy uzasadnianego rozdziału co do zasady pełnią rolę techniczno-legislacyjną i mają na celu zmianę nazwy organu z Generalnego Inspektora Ochrony Danych Osobowych na Prezesa Urzędu Ochrony Danych Osobowych, administratora bezpieczeństwa informacji na inspektora ochrony danych oraz odwołują odwołania do obowiązującej ustawy.

Projektodawca w przepisach zmieniających zdecydował się utrzymać szczególną pozycję Prezesa Urzędu Ochrony Danych Osobowych jako organu o zagwarantowanej autonomii budżetowej stosownie do art. 139 ust. 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Mimo że Prezes Urzędu nie jest organem konstytucyjnym, wymóg zapewnienia

organowi autonomii budżetowej wynika wprost z rozporządzenia 2016/679. Zgodnie z art. 52 ust. 6 rozporządzenia 2016/679 „każde państwo członkowskie zapewnia, by każdy organ nadzorczy podlegał kontroli finansowej w sposób nienaruszający jego niezależności oraz dysponował odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego". W ocenie projektodawcy, w polskim systemie prawnym powyższy wymóg może być zagwarantowany właśnie autonomią budżetową, a więc poprzez utrzymanie w tym zakresie pozycji posiadanej obecnie przez GIODO.

Projektowana zmiana w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524) ma na celu utrzymanie istniejącego stanu rzeczy i zachowanie możliwości przetwarzania przez Najwyższą Izbę Kontroli danych, w tym danych szczególnie chronionych, takich samych jak w obowiązującej ustawie. Wprowadzenie zmiany polega na dostosowaniu wykorzystywanych w ustawie sformułowań do przewidzianych w rozporządzeniu 2016/679.

Rozdział 14. Przepisy przejściowe i dostosowujące.

Projektodawca, zapewniając sprawność działania systemu ochrony danych osobowych oraz dostrzegając ogromny wpływ na jego działania inspektorów ochrony danych, zdecydował się wprowadzić przepisy przejściowe w tym zakresie. Dostrzegając trudność w możliwości zgłoszenia wszystkich osób pełniących dotychczas funkcję administratorów bezpieczeństwa informacji jako inspektorów ochrony danych, osoby pełniące funkcję administratorów bezpieczeństwa informacji będą miały na to czas do 1 września 2018 r. Trudność w dokonaniu takiego zgłoszenia w dniu 25 maja może powstać zarówno po stronie administratorów, jak i Prezesa Urzędu, który otrzymałby ogromną liczbę nowych zgłoszeń w stosunkowo krótkim czasie. W ocenie projektodawcy nie jest jednak możliwe przesądzenie, że wszystkie osoby pełniące funkcję administratorów bezpieczeństwa informacji stają się z datą wejścia w życie projektowanej ustawy inspektorami ochrony danych, z uwagi na dużą liczbę nowych obowiązków wynikających z rozporządzenia 2016/679. Wymaga ona podjęcia świadomej decyzji po stronie osoby chcącej pełnić funkcję inspektora ochrony danych.

Projektodawca, przewidując w projekcie ustanowienie organu – Prezesa Urzędu Ochrony Danych Osobowych, widzi również konieczność zapewnienia pełnej ciągłości działania organu. W związku z powyższym projektowane przepisy przewidują, że z dniem wejścia w życie ustawy pracownicy zatrudnieni w Biurze Generalnego Inspektora Ochrony Danych Osobowych stają się pracownikami Urzędu Ochrony Danych Osobowych, mienie Skarbu

Państwa będące we władaniu Biura Generalnego Inspektora Ochrony Danych Osobowych staje się mieniem będącym we władaniu Urzędu Ochrony Danych Osobowych, a należności i zobowiązania Biura Generalnego Inspektora Ochrony Danych Osobowych z dniem wejścia w życie ustawy stają się należnościami i zobowiązaniami Biura Urzędu Ochrony Danych Osobowych. Przepisy projektu wskazują bardzo wyraźnie, że Generalny Inspektor Ochrony Danych Osobowych staje się Prezesem Urzędu Ochrony Danych Osobowych i pełni swoją funkcję do czasu upływu kadencji, na którą został powołany. Tym samym w projekcie nie przewiduje się jakiegokolwiek skrócenia kadencji osoby obecnie pełniącej funkcję GIODO. W Polsce osoba pełniąca funkcję GIODO została powołana na to stanowisko przez Sejm RP w dniu 9 kwietnia 2015 r., a Senat zaakceptował ten wybór w dniu 16 kwietnia 2015 r. Natomiast od dnia złożenia ślubowania przed Sejmem, tj. od dnia 22 kwietnia 2015 r., zgodnie z obowiązującą ustawą o ochronie danych osobowych, rozpoczęła się czteroletnia kadencja GIODO. Kadencja organu upłynie więc w kwietniu 2019 r.

Rozdział 15. Przepisy końcowe.

Przepisy projektowanego rozdziału przewidują zgodnie z zasadami poprawnej legislacji maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy w okresie 10-letnim od wejścia w życie projektowanej ustawy.

Przewiduje się, że projektowana ustawa wejdzie w życie z dniem 25 maja 2018 r.

Projekt ustawy będzie miał wpływ na sytuację małych i średnich przedsiębiorców. Należy w tym zakresie wskazać na przyznane Prezesowi Urzędu uprawnienie do wydawania rekomendacji w obszarze zasad zabezpieczania danych osobowych, wypracowywanych z przedsiębiorcami, w tym należących do małych i średnich przedsiębiorstw. Zgodnie z treścią projektu, monitorowaniem przestrzegania zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 Rozporządzenia, zajmuje się podmiot akredytowany przez Prezesa Urzędu. Podmiotem takim mogą być przedsiębiorcy, w tym mali i średni. Obliczenia zostały podjęte na podstawie dołączonej do projektu Oceny Skutków Regulacji. Od dnia 25 maja 2018 r. będzie istniała przewidziana Rozporządzeniem możliwość nałożenia na przedsiębiorców administracyjnych kar finansowych za naruszenie przepisów o ochronie danych osobowych w przypadku nałożenia kary przez Prezesa Urzędu. Trudno w tej chwili oszacować skutki takiego przepisu.

Projekt ustawy o ochronie danych osobowych jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

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 ustawy został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny", oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248). W trybie przepisów ww. ustawy nie wpłynęły wnioski.

Nazwa projektu Projekt ustawy o ochronie danych osobowych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Marek Zagórski – Sekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Dr Maciej Kawecki, Dyrektor Departamentu Zarządzania Danymi w Ministerstwie Cyfryzacji maciej.kawecki@mc.gov.pl	**Data sporządzenia** 27.03.2018 r. **Źródło:** 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 **Nr w wykazie prac UC 101**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

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 (dalej: rozporządzenie 2016/679). Ministerstwo Cyfryzacji jest resortem odpowiedzialnym za zapewnienie skutecznego stosowania rozporządzenia w polskiej przestrzeni prawnej przez przyjęcie właściwej ustawy krajowej zastępującej obowiązującą obecnie ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922), dalej: „ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych", oraz zmianę właściwych przepisów sektorowych. Organem właściwym do przygotowania nowej regulacji prawnej w zakresie ochrony danych osobowych jest minister właściwy do spraw informatyzacji, gdyż do jego zadań, zgodnie z art. 12a ust. 1 pkt 8 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2016 r., poz. 2260, z późn. zm.) należą sprawy kształtowania polityki państwa w zakresie ochrony danych osobowych. **Rozporządzenie 2016/679 zacznie być aktem bezpośrednio stosowanym oraz bezpośrednio skutecznym 25 maja 2018 r. i do tego czasu każde z państw członkowskich zobowiązane jest do zapewnienia jego skutecznego stosowania w swoim porządku prawnym poprzez przyjęcie właściwych przepisów wewnętrznych.** W ramach realizacji tej kompetencji Minister Cyfryzacji przygotował projekt nowej ustawy o ochronie danych osobowych oraz zmian w przepisach sektorowych wprowadzanych projektem ustawy wprowadzającej ustawę o ochronie danych osobowych. Podjęte działania legislacyjne zgodnie z zasadami prawa Unii Europejskiej opierały się na założeniu, że nowa ustawa o ochronie danych osobowych będzie zawierała wyłącznie przepisy, które zostały przez prawodawcę unijnego wprost przekazane do uregulowania w prawie krajowym, oraz takie, w których rozporządzenie 2016/679 pozostawiło pewną swobodę regulacyjną poszczególnym państwom członkowskim. W szczególności przedmiotem nowej ustawy o ochronie danych osobowych są kwestie dotyczące krajowego organu nadzorczego, postępowania przed tym organem, postępowania kontrolnego, wieku dziecka wymaganego do samodzielnego wyrażania zgody na przetwarzanie danych osobowych w odniesieniu do usług społeczeństwa informacyjnego, certyfikacji, sądowej ochrony praw przysługujących. Jednym z zagadnień, które musi być rozwiązane w związku z reformą systemu ochrony danych osobowych, jest zapewnienie efektywniejszego od obowiązującego obecnie systemu ochrony danych osobowych. Według informacji uzyskanych przez Ministra Cyfryzacji w związku z analizą wyroków wydawanych przez Naczelny Sąd Administracyjny w 2015 r. spośród spraw, które trafiły do sądów, średni czas trwania postępowania w sprawach dotyczących zasad naruszenia ochrony danych osobowych w Polsce wynosi 295 dni do czasu wydania przez Generalnego Inspektora Ochrony Danych Osobowych decyzji w I instancji, a do decyzji w II instancji – 437 dni. Nie lepiej jest w momencie, gdy czeka się na uzyskanie prawomocnego orzeczenia w sprawie dot. ochrony danych osobowych. Tutaj zainteresowany czeka średnio 600 dni. Wskazane statystyki pokazują ogromną skalę problemu, z którą mamy do czynienia. W 2015 r. prowadzone były postępowania (takimi statystykami dysponujemy), gdy obywatel do czasu uzyskania prawomocnego wyroku w sprawie czekał ponad 1600 dni, a więc ponad 4 lata. Założeniem przyświecającym Ministrowi Cyfryzacji w zapewnieniu skutecznego stosowania rozporządzenia 2016/679 w polskiej przestrzeni prawnej jest przyśpieszenie trwających postępowań poprzez utrzymanie terminów wynikających z ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257); zasadą jest wydanie rozstrzygnięcia niezwłocznie. W swoim piśmie z dnia 26 czerwca 2017 r. do Generalnego Inspektora Ochrony Danych Osobowych Rzecznik Praw Obywatelskich wskazał, że *do Biura Rzecznika Praw Obywatelskich napływają regularne skargi, w których obywatele wskazują na opieszałość organu ochrony danych osobowych, długotrwałe rozpoznawanie spraw i kilkuletnie oczekiwanie na wydanie decyzji przez GIODO. O konkretnych indywidualnych sprawach RPO informuje Biuro GIODO w trybie ustawy o RPO, prosząc na bieżąco o informacje i wyjaśnienia. Obywatele mają bowiem prawo oczekiwać, że ich sprawy będą rozpatrywane bez zbędnej zwłoki, zgodnie z kpa.* Na podobne problemy w funkcjonowaniu polskiego systemu ochrony danych osobowych uwagę wskazywała również Helsińska Fundacja Praw Człowieka w swoim raporcie dotyczącym mechanizmów dochodzenia ochrony w zakresie danych osobowych w Polsce. Sam Generalny Inspektor Ochrony Danych Osobowych na swojej stronie internetowej udostępnił komunikat, w którym