Warszawa, dnia 14 września 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

DP-WLI.0211.2.2017

Według rozdzielnika

Szanowni Państwo

stosownie do art. 19 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2015 r. poz. 1881) w załączeniu przesyłam ***projekt ustawy - Przepisy wprowadzające ustawę o ochronie danych osobowych*** oraz ***projekt ustawy o ochronie danych osobowych.***

Projekty ustaw wpisane zostały do Wykazu prac legislacyjnych Rady Ministrów pod numerem UC100 i UC101.

Zwracam się z prośbą o zaopiniowanie ww. projektów w terminie 30 dni od otrzymania pisma. Jednocześnie uprzejmie informuję, że brak stanowiska w wyznaczonym terminie potraktowany zostanie jako akceptacja projektów.

Uwagi w wersji edytowalnej proszę przekazywać także na adres: konsultacje.odo@mc.gov.pl

Z poważaniem,
Anna Streżyńska
Minister Cyfryzacji
/-podpisano elektronicznie/

Otrzymują:
1. Business Centre Club – Związek Pracodawców
2. NSZZ „Solidarność”
3. Ogólnopolskie Porozumienie Związków Zawodowych
4. Federacja Związków Zawodowych
5. Pracodawcy RP
6. Związek Rzemiosła Polskiego
7. Konfederacja Lewiatan

Projekt z dnia 12 września 2017 r.

U S T A W A

z dnia …….. 2017 r.

o ochronie danych osobowych[1)]

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 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 4.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679".

2. Ustawa określa:

1) podmioty obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o wyznaczaniu;
2) warunki i tryb udzielania certyfikacji i akredytacji;
3) organ właściwy w sprawie ochrony danych osobowych;
4) postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;
5) europejską współpracę administracyjną;
6) postępowanie kontrolne;
7) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych;
8) administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

[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 osobowych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1)

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.[2])) a także do działalności literackiej lub artystycznej nie stosuje się przepisów art. 5 – 9, 11, 13 - 16, 18 -22, 27, 28 ust. 2 – 10 i art. 30 rozporządzenia 2016/679.

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

3. Jeżeli ograniczenia o których mowa w ust. 1 i 2 różnią się zależnie od państwa członkowskiego, zastosowanie powinno mieć prawo państwa członkowskiego, któremu podlega administrator.

Art. 3. W przypadku usług świadczonych drogą elektroniczną oferowanych bezpośrednio osobie, która nie ukończyła lat trzynastu i która przebywa na terytorium Rzeczpospolitej Polskiej, gdy podstawą przetwarzania danych osobowych jest zgoda tej osoby, przetwarzanie danych osobowych możliwe jest wyłącznie po uzyskaniu uprzedniej zgody jej przedstawiciela ustawowego albo po niezwłocznym potwierdzeniu przez przedstawiciela ustawowego zgody wyrażonej przez taką osobę.

Rozdział 2

Inspektorzy ochrony danych

Art. 4. Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się organy publiczne wskazane w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23, 868, 996, 1579 i 2138 oraz z 2017 r. poz. 935)

[2)] 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 oraz z 2013 r. poz. 771.

oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870, z późn. zm.[3]).

Art. 5. 1 Administrator danych albo podmiot przetwarzający, który wyznaczył inspektora ochrony danych, zwanego dalej „inspektorem", zawiadamia Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu", o jego wyznaczeniu, w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

2. W zawiadomieniu administrator danych albo podmiot przetwarzający obowiązany jest wskazać adres i pełną nazwę, a w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna – miejsce zamieszkania oraz imię i nazwisko.

3. O każdej zmianie danych, o której mowa w ust. 1 i 2, w tym o odwołaniu inspektora, należy zawiadomić Prezesa Urzędu w terminie 14 dni od dnia zaistnienia zmiany.

4. Zawiadomienia, o których mowa w ust. 1 i 3, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.

5. Prezes Urzędu prowadzi system teleinformatyczny umożliwiający przesyłanie zawiadomień w postaci elektronicznej.

6. Prezes Urzędu prowadzi wewnętrzną ewidencję zawiadomień, o których mowa w ust. 1 i 3. Ewidencja zawiera dane, o których mowa w ust. 1 i 2.

Rozdział 3

Certyfikacja i akredytacja

Art. 6. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, dokonuje Prezes Urzędu.

Art. 7. Prezes Urzędu opracowuje kryteria certyfikacji i udostępnia je w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

Art. 8.1. Certyfikacji dokonuje się na wniosek administratora lub podmiotu przetwarzającego.

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2016 r. poz. 1948, 1984 i 2260 oraz z 2017 r. poz. 60, 191, 659, 933, 935 i 1089.

2. Wniosek o certyfikację zawiera co najmniej:

1) nazwę administratora lub podmiotu przetwarzającego albo jego imię i nazwisko oraz wskazanie siedziby lub adresu zamieszkania administratora lub podmiotu przetwarzającego;
2) informacje potwierdzające spełnianie kryteriów certyfikacji.

3. Do wniosku dołącza się dokumenty potwierdzające spełnienie kryteriów certyfikacji albo ich elektroniczne kopie.

4. Wniosek składa się w postaci papierowej albo elektronicznej. Wniosek w postaci papierowej opatruje się podpisem własnoręcznym, natomiast wniosek w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Art. 9.1. Prezes Urzędu rozpatruje wniosek o certyfikację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia wniosku, zawiadamia wnioskodawcę o udzieleniu lub odmowie udzielenia certyfikacji.

2. Odmowa udzielenia certyfikacji następuje w drodze decyzji w przypadku stwierdzenia, że administrator lub podmiot przetwarzający nie spełnia kryteriów certyfikacji.

3. Do decyzji, o której mowa w ust. 2, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 53 i 55.

Art. 10.1. Dokumentem potwierdzającym certyfikację jest certyfikat.

2. Certyfikat zawiera co najmniej:

1) oznaczenie administratora lub podmiotu przetwarzającego;
2) nazwę organu udzielającego certyfikacji oraz wskazanie adresu jego siedziby;
3) numer i oznaczenie certyfikatu;
4) okres, na jaki została udzielona certyfikacja;
5) datę wydania i podpis Prezesa Urzędu lub osoby przez niego upoważnionej.

Art. 11. W okresie, na jaki została udzielona certyfikacja administrator lub podmiot przetwarzający są obowiązani spełniać kryteria certyfikacji.

Art. 12. Prezes Urzędu prowadzi publicznie dostępny wykaz administratorów i podmiotów przetwarzających, którym udzielono certyfikacji.

Art. 13.1 Prezes Urzędu w terminie, o którym mowa w art. 9 ust. 1, a także po udzieleniu certyfikacji jest uprawniony do przeprowadzenia czynności sprawdzających u administratora lub podmiotu przetwarzającego w celu oceny spełniania przez ten podmiot kryteriów certyfikacji.

2. Prezes Urzędu zawiadamia 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 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 upoważnienia wydanego przez Prezesa Urzędu, które zawiera:

1) imię i nazwisko osoby przeprowadzającej czynności sprawdzające;
2) oznaczenie administratora lub podmiotu przetwarzającego;
3) zakres czynności sprawdzających.

Art. 14.1. Osoba przeprowadzająca czynności sprawdzające jest uprawniona do:

1) wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń;
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) uzyskania ustnych lub pisemnych wyjaśnień w sprawach związanych z działalnością objętą certyfikacją.

2. Czynności sprawdzających dokonuje się w obecności administratora, podmiotu przetwarzającego lub osoby przez niego upoważnionej.

3. Z czynności sprawdzających sporządza się protokół i przedstawia administratorowi lub podmiotowi przetwarzającemu. Przepis art. 72 stosuje się odpowiednio.

Art. 15.1. Prezes Urzędu w drodze decyzji cofa udzieloną certyfikację w przypadkach, o których mowa w art. 42 ust. 7 rozporządzenia 2016/679.

2. W decyzji, o której mowa w ust.1, Prezes Urzędu wskazuje przyczyny cofnięcia certyfikacji.

3. Do decyzji, o której mowa w ust.1, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 53 i 55.

Art. 16.1. Za czynności związane z postępowaniem o udzielenie certyfikacji Prezes Urzędu pobiera opłatę w wysokości trzykrotności przeciętnego miesięcznego wynagrodzenia za pracę w gospodarce narodowej w roku poprzednim ogłaszanego przez Prezesa Głównego Urzędu Statystycznego.

2. Opłaty, o których mowa w ust. 1, stanowią dochód budżetu państwa.

Art. 17. Monitorowaniem przestrzegania zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, zajmuje się podmiot akredytowany przez Prezesa Urzędu zgodnie z kryteriami określonymi w art. 41 ust. 2 rozporządzenia 2016/679.

Art. 18.1. Akredytacji podmiotu ubiegającego się o monitorowanie przestrzegania zatwierdzonego kodeksu postepowania dokonuje się na wniosek.

2. Wniosek o akredytację zawiera co najmniej:

1) nazwę wnioskodawcy oraz wskazanie adresu jego siedziby;
2) informacje potwierdzające spełnienie kryteriów, o których mowa w art. 41 ust. 2 rozporządzenia 2016/679.

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

4. Wniosek składa się w postaci papierowej albo elektronicznej. Wniosek w postaci papierowej opatruje się podpisem własnoręcznym, natomiast wniosek w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

5. Prezes Urzędu rozpatruje wniosek o akredytację i w terminie nie dłuższym niż 3 miesiące od dnia złożenia kompletnego wniosku, zawiadamia wnioskodawcę o udzieleniu lub odmowie udzielenia akredytacji.

6. Odmowa udzielenia akredytacji następuje w drodze decyzji w przypadku stwierdzenia, że wnioskodawca nie spełnia kryteriów, o których mowa w art. 41 ust. 2 rozporządzenia 2016/679.

7. Do decyzji, o której mowa w ust. 6, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 53 i 55.

Art. 19.1. Dokumentem potwierdzającym akredytację jest certyfikat akredytacyjny.

2. Certyfikat akredytacyjny zawiera co najmniej:

1) oznaczenie organu udzielającego akredytacji i adres jego siedziby;
2) oznaczenie podmiotu akredytowanego i adres jego siedziby;
3) numer i oznaczenie certyfikatu akredytacyjnego;
4) okres, na jaki została udzielona akredytacja;
5) datę wydania i podpis Prezesa Urzędu lub osoby przez niego upoważnionej.

3. W okresie, na jaki została udzielona akredytacja podmiot akredytowany jest obowiązany spełniać kryteria akredytacji.

4. Prezes Urzędu prowadzi wykaz podmiotów akredytowanych i udostępnia go w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

5. W przypadku, gdy podmiot akredytowany:

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

- Prezes Urzędu w drodze decyzji cofa udzieloną akredytację.

6. Do decyzji, o której mowa w ust. 5, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 53 i 55.

Rozdział 4

Prezes Urzędu Ochrony Danych Osobowych

Art. 20.1. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych.

2. Prezes Urzędu jest organem nadzorczym w rozumieniu rozporządzenia 2016/679 i organem nadzorczym 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 uchylająca decyzję ramową Rady 2008/977/WSiSW** (Dz. Urz. UE L 119 z 4.5.2016, s. 89).

3. Prezesa Urzędu powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu na wniosek Prezesa Rady Ministrów.

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

1) jest obywatelem polskim;
2) posiada tytuł naukowy doktora;
3) posiada wiedzę z zakresu ochrony danych osobowych;
4) przez okres co najmniej pięciu lat wykonywała czynności bezpośrednio związane z ochroną danych osobowych;
5) korzysta z pełni praw publicznych;
6) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.

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

6. Kadencja Prezesa Urzędu trwa 4 lata od dnia złożenia ślubowania.

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;
3) sprzeniewierzył się ślubowaniu;
4) został skazany prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego.

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

Art. 21. Przed przystąpieniem do wykonywania obowiązków Prezes Urzędu składa przed Sejmem następujące ślubowanie:

„Obejmując stanowisko Prezesa Urzędu Ochrony Danych Osobowych uroczyście ślubuję dochować wierności postanowieniom Konstytucji Rzeczypospolitej Polskiej, strzec prawa do ochrony danych osobowych kierując się przepisami prawa oraz zasadami współżycia społecznego i sprawiedliwości. Ślubuję, że powierzone mi obowiązki

wypełniać będę bezstronnie, z najwyższą sumiennością i starannością, że będę strzec godności powierzonego mi stanowiska.”.

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

Art. 22.1. Prezes Urzędu może wykonywać swoje zadania przy pomocy do trzech zastępców Prezesa Urzędu.

2. Na wniosek ministra właściwego do spraw informatyzacji Prezes Rady Ministrów może powołać dwóch zastępców Prezesa Urzędu. Odwołanie zastępcy Prezesa Urzędu następuje w tym samym trybie.

3. Na wniosek ministra właściwego do spraw wewnętrznych Prezes Rady Ministrów powołuje zastępcę Prezesa Urzędu.

4. Wniosek, o którym mowa w ust. 3, minister właściwy do spraw wewnętrznych przekazuje celem zaopiniowania Ministrowi Sprawiedliwości, Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw finansów publicznych oraz Prokuratorowi Generalnemu.

5. Odwołanie zastępcy Prezesa Urzędu powołanego na wniosek ministra właściwego do spraw wewnętrznych następuje w trybie, o którym mowa w ust. 3 i 4.

6. Na zastępcę Prezesa Urzędu może być powołana osoba, która przez okres co najmniej czterech lat wykonywała czynności bezpośrednio związane z ochroną danych osobowych i spełnia warunki, o których mowa w art. 20 ust. 4 pkt 1, 3, 5 i 6.

Art. 23.1. Prezes Urzędu nie może zajmować innego stanowiska, z wyjątkiem stanowiska 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 nie może należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.

3. Przepisy ust. 1 i 2 stosuje się odpowiednio do zastępców Prezesa Urzędu.

Art. 24.1. Prezes Urzędu nie może być bez uprzedniej zgody Sejmu 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 2015 r. poz. 1094, 1485, 1634 i 1707 oraz z 2017 r. poz. 966), 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 2016 r. poz. 1713 i 1948 oraz z 2017 r. poz. 708, 962 i 966), 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. 25. Przedawnienie w postępowaniu karnym czynu objętego immunitetem nie biegnie w okresie korzystania z immunitetu.

Art. 26.1. 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. 27.1. 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. 26 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. 26 ust. 3 i 4, Marszalek 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 rozpatrzenia wniosku. Pomiędzy doręczeniem powiadomienia a terminem rozpatrzenia wniosku, o ile nie zachodzi wypadek nie cierpiący zwłoki, powinno upłynąć co najmniej 7 dni.

5. Na żądanie organu właściwego do rozpatrzenia wniosku sąd albo odpowiedni organ, przed którym toczy się postepowanie 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 sprawozdania, o którym mowa w ust. 7, Prezesowi Urzędu przysługuje prawo zabrania głosu.

9. Sejm 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. 28.1. Zakaz zatrzymania, o którym mowa w art. 24, obejmuje wszelkie formy pozbawienia lub ograniczenia wolności osobistej Prezesa Urzędu przez organy sprawujące przymus.

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. 27 ust. 1 – 8 stosuje się odpowiednio.

5. Sejm 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 nie dotyczy wykonania kary pozbawienia wolności orzeczonej prawomocnym wyrokiem sądu.

Art. 29. 1. Marszałek Sejmu przesyła wnioskodawcy niezwłocznie uchwałę, o której mowa w art. 27 ust. 9 i art. 28 ust. 5.

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

Art. 30. Przepisy ustawy dotyczące odpowiedzialności karnej Prezesa Urzędu stosuje się odpowiednio do odpowiedzialności za wykroczenia.

Art. 31. **Szczegółowy tryb postępowania w sprawach, o których mowa w art. 25 – 30, określa Regulamin Sejmu.**

Art. 32.1. Prezes Urzędu wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych, zwanego dalej „Urzędem”.

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

1) organizację 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. 33.1. 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 tajemnicy służbowej nie może być ograniczony w czasie i trwa także po zakończeniu kadencji albo zatrudnienia.

Art. 34.1. Przy Prezesie Urzędu działa Rada do Spraw Ochrony Danych Osobowych, zwana dalej „Radą”. Rada 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. 7;
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 w Biuletynie Informacji Publicznej na stronie podmiotowej 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 mogą rekomendować:

1) członkowie Rady Ministrów;
2) Rzecznik Praw Obywatelskich;
3) Prezes Głównego Urzędu Statystycznego;
4) Prezes Urzędu Komunikacji Elektronicznej;
5) Prezes Urzędu Ochrony Konkurencji i Konsumentów;
6) Naczelny Dyrektor Archiwów Państwowych;
7) izby gospodarcze;

8) jednostki naukowe w rozumieniu przepisów ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (Dz. U. z 2016 r., poz. 2045, z późn. zm.[4])));
9) stowarzyszenia wpisane do Krajowego Rejestru Sądowego, których celem statutowym jest działalność na rzecz ochrony danych osobowych.

8. Rekomendowany do Rady kandydat powinien posiadać wykształcenie wyższe oraz wyrazić zgodę na kandydowanie.

9. Prezes Urzędu powołuje skład Rady na dwuletnią kadencję spośród kandydatów rekomendowanych przez podmioty, o których mowa w ust. 7.

10. 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.

11. W przypadkach, o których mowa w ust. 10, Prezes Urzędu powołuje na członka Rady osobę spośród pozostałych rekomendowanych kandydatów po sprawdzeniu aktualności rekomendacji.

12. Prezes Urzędu powołuje i odwołuje Przewodniczącego i Wiceprzewodniczącego Rady spośród jej członków.

13. Przewodniczący Rady kieruje jej pracami i reprezentuje ją na zewnątrz. W przypadku nieobecności Przewodniczącego zastępuje go Wiceprzewodniczący.

14. Obsługę Rady zapewnia Urząd.

15.Na posiedzenie Rady mogą być zapraszane, przez Prezesa Urzędu oraz Przewodniczącego Rady, inne osoby, o ile jest to wskazane dla realizacji zadań Rady.

16. Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość wynagrodzenia członka Rady za udział w posiedzeniu, uwzględniając funkcje pełnione przez członków Rady i zakres obowiązków członków Rady, a także mając na uwadze, że wynagrodzenie za jedno posiedzenie Rady nie może przekroczyć 50% minimalnego wynagrodzenia określonego na

---

[4)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2016 r. poz.2260 oraz z 2017 r. poz. 859, 1475, 1530 i 1556.

podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. z 2017 r. poz. 847), obowiązującego w dniu powołania Rady.

17. Zamiejscowym członkom Rady przysługują diety oraz zwrot kosztów podróży i zakwaterowania na warunkach określonych w przepisach wydanych na podstawie art. 775 § 2 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2016 r., poz. 1666, 2138 i 2255 oraz z 2017 r. poz. 60 i 962).

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

Art. 35. Prezes Urzędu, do dnia 31 sierpnia przedstawia Sejmowi, Prezesowi Rady 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.

Art. 36. Prezes Urzędu opiniuje założenia i projekty aktów prawnych dotyczące ochrony danych osobowych.

Art. 37.1. 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 bądź 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. 38. Prezes Urzędu udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej:

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.

Art. 39. 1. Prezes Urzędu ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679.

2. Komunikat, o którym mowa w ust. 1, ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

Art. 40. Prezes Urzędu w procedurze uprzednich konsultacji może zawiesić bieg terminów, o których mowa w art. 36 ust. 2 rozporządzenia 2016/679, jednokrotnie i na okres nie przekraczający 14 dni.

Art. 41. Prezes Urzędu prowadzi system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679.

Art. 42.1.Prezes Urzędu w drodze decyzji:

1) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 rozporządzenia 2016/679;
2) zatwierdza kodeks postępowania, o którym mowa w art. 40 rozporządzenia 2016/679;
3) przyjmuje standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit d rozporządzenia 2016/679;
4) udziela zezwolenia, o którym mowa w art. 46 ust. 3 rozporządzenia 2016/679.

2. Do decyzji, o których mowa w ust. 1, przepisy rozdziału o postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się odpowiednio, z wyłączeniem art. 53 i 55.

Art. 43.1. Prezes Urzędu opracowuje i udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.

2. Rekomendacje sporządzane są z uwzględnieniem specyfiki danego rodzaju działalności i podlegają okresowej aktualizacji.

3. Projekt rekomendacji Prezes Urzędu konsultuje z zainteresowanymi podmiotami, których zakresu działania dotyczy dany projekt.

Rozdział 5

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

Art. 44.1. Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem”, jest prowadzone przez Prezesa Urzędu.

2. Postępowanie jest postępowaniem jednoinstancyjnym.

Art. 45. Gdy prawa osoby przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, organizacja społeczna może występować z żądaniem:

1) wszczęcia postępowania,

2) dopuszczenia jej do udziału w postępowaniu,

jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes osoby, której prawa zostały naruszone.

Art. 46. O każdym przypadku niezałatwienia sprawy w terminie Prezes Urzędu jest obowiązany zawiadomić strony, podając przyczyny zwłoki, informację o stanie sprawy i przeprowadzonych w jej toku czynnościach oraz wskazując nowy termin załatwienia sprawy.

Art. 47.1. Prezes Urzędu może wyznaczyć stronie termin do przedstawienia dowodu będącego w jej posiadaniu.

2. Termin ustala się uwzględniając charakter dowodu i stan postępowania, przy czym nie może on być krótszy niż 7 dni.

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

Art. 48.1. Prawo Prezesa Urzędu do dostępu do wszelkich informacji, w tym danych osobowych, niezbędnych Prezesowi Urzędu do realizacji zadań podlega ograniczeniu ze względu na tajemnice ustawowo chronione.

2. Wykonywanie prawa, o którym mowa w ust. 1, jest możliwe na zasadach określonych w przepisach regulujących dostęp do tajemnic ustawowo chronionych.

Art. 49.1. Strona może zastrzec informacje, dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa, dostarczane Prezesowi Urzędu.

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

3. 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. 50.1. Prezes Urzędu na wniosek lub z urzędu może, w drodze postanowienia, w niezbędnym zakresie ograniczyć prawo wglądu do materiału dowodowego, jeżeli udostępnienie tego materiału groziłoby ujawnieniem tajemnicy przedsiębiorstwa, lub innych tajemnic podlegających ochronie na podstawie odrębnych przepisów.

2. Wniosek o ograniczenie prawa wglądu do materiału dowodowego składa się do Prezesa Urzędu wraz z uzasadnieniem oraz wersją dokumentu niezawierającą informacji objętych ograniczeniem, o którym mowa w ust. 1, ze stosowną adnotacją.

3. Jeżeli wniosek nie spełnia wymagań określonych w ust. 2, Prezes Urzędu wzywa wnioskodawcę do jego uzupełnienia w wyznaczonym terminie. W przypadku nieprzedłożenia w wyznaczonym terminie wersji dokumentu, o której mowa w ust. 2, wniosek pozostawia się bez rozpoznania.

4. Stronom udostępnia się materiał dowodowy niezawierający informacji objętych ograniczeniem, o którym mowa w ust. 1, ze stosowną adnotacją.

5. Obowiązku złożenia wersji dokumentu niezawierającej informacji objętych ograniczeniem, o którym mowa w ust. 1, nie stosuje się w sytuacji gdy cały dokument jest objęty ograniczeniem, o którym mowa w ust. 1.

Art. 51.1. Kto, będąc obowiązany do osobistego stawienia się mimo prawidłowego wezwania nie stawił się bez uzasadnionej przyczyny jako świadek lub biegły albo bezzasadnie odmówił złożenia zeznania, przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej, może być ukarany karą grzywny do 500 zł. Na postanowienie o ukaraniu służy skarga do sądu administracyjnego.

2. Prezes Urzędu na wniosek ukaranego, złożony w ciągu 7 dni od daty doręczenia postanowienia o ukaraniu, może uznać za usprawiedliwioną nieobecność lub odmowę zeznania, wydania opinii albo okazania przedmiotu oględzin i zwolnić od kary grzywny. Na postanowienie o odmowie zwolnienia od kary grzywny służy skarga do sądu administracyjnego.

Art. 52. W toku postępowania może być prowadzone postępowanie kontrolne, o którym mowa w rozdziale 7.

Art. 53.1. 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. Przepisu art. 10 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego nie stosuje się.

2. W postanowieniu, o którym mowa w ust. 1, Prezes Urzędu określa czas jego obowiązywania. Postanowienie to obowiązuje nie dłużej niż do czasu wydania decyzji kończącej postępowanie w sprawie.

Art. 54. Prezes Urzędu wydaje decyzję o umorzeniu postępowania gdy żądanie wszczęcia postępowania zostało wniesione w sprawie, która jest przedmiotem postępowania toczącego się przed Prezesem Urzędu.

Art. 55.1. W przypadku naruszenia przepisów o ochronie danych osobowych Prezes Urzędu, w drodze decyzji podejmuje rozstrzygnięcia, o których mowa w art. 58 ust. 2 lit. b-j rozporządzenia 2016/679.

2. Uzasadnienie faktyczne decyzji nakładającej administracyjną karę pieniężną poza elementami, o których mowa w art. 107 ust. 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, zawiera wskazanie przesłanek z art. 83 ust. 2 rozporządzenia 2016/679, na których Prezes Urzędu oparł się nakładając administracyjną karę pieniężną oraz ustalając jej wysokość.

Art. 56. W przypadku gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia Prezes Urzędu może, w drodze decyzji udzielić upomnienia.

Art. 57.1. W przypadku podjęcia przez Prezesa Urzędu w drodze decyzji rozstrzygnięć, o których mowa w art. 58 ust. 2 lit. b – g i lit. j rozporządzenia 2016/679, wobec organów, o których mowa w art. 5 § 2 pkt 3 Kodeksu postępowania administracyjnego albo podmiotów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, Prezes Urzędu udostępnia prawomocne decyzje w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

2. Do udostępniania decyzji, o których mowa w ust. 1, stosuje się przepisy art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764 i z 2017 r. poz. 933).

3. Organy, o których mowa w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego a także podmioty publiczne, o których mowa w art. 9 ustawy

z dnia 27 sierpnia 2009 r. o finansach publicznych, niezwłocznie udostępniają na swoich stronach internetowych informacje o działaniach podjętych w celu wykonania decyzji, o których mowa w ust. 1.

Art. 58. Decyzje Prezesa Urzędu, o których mowa w art. 55 ust. 1, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa.

Art. 59.1. Decyzje wydane przez Prezesa Urzędu podlegają natychmiastowemu wykonaniu.

2. Wniesienie przez stronę skargi do sądu administracyjnego powoduje wstrzymanie wykonania decyzji w zakresie dotyczącym administracyjnej kary pieniężnej.

Art. 60. Postanowienia wydane przez Prezesa Urzędu strona może zaskarżyć w skardze na decyzję Prezesa Urzędu.

Art. 61 W sprawach nieuregulowanych w ustawie do postępowania przed Prezesem Urzędu stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyłączeniem przepisów art. 66a.

Rozdział 6

Europejska współpraca administracyjna

Art. 62. W przypadkach określonych w art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 rozporządzenia 2016/679, Prezes Urzędu może wydać postanowienie, o którym mowa w art. 53 ust. 1.

Art. 63.1. Wszelkie informacje kierowane przez Prezesa Urzędu do organów nadzorczych innych państw członkowskich w ramach europejskiej współpracy administracyjnej, powinny zostać przetłumaczone na jeden z języków urzędowych tego państwa członkowskiego lub na język angielski.

2. Wszelkie informacje kierowane do Prezesa Urzędu w związku z europejską współpracą administracyjną powinny zostać przetłumaczone na język polski.

Art. 64.1. 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.

2. Okresy, w których pracownicy organu nadzorczego innego państwa członkowskiego Unii Europejskiej przebywają na terytorium Rzeczypospolitej Polskiej, biorąc udział we wspólnej operacji, nie są uważane za okresy pobytu wpływające na zmianę miejsca zamieszkania dla celów opodatkowania podatkiem dochodowym zgodnie z prawem Rzeczypospolitej Polskiej.

Rozdział 7

Postępowanie kontrolne

Art. 65.1. Prezes Urzędu może prowadzić kontrole przestrzegania przepisów o ochronie danych osobowych.

2. Postępowanie kontrolne może być prowadzone zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli bądź poza planem na podstawie uzyskanych przez Prezesa Urzędu informacji albo przeprowadzonych analiz.

Art. 66.1. Kontrola może być przeprowadzona przez upoważnionego pracownika Urzędu, zwanego dalej „kontrolującym”.

2. Do przeprowadzania kontroli Prezes Urzędu może upoważnić członka lub pracownika organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 rozporządzenia 2016/679.

Art. 67.1. Kontrolujący podlega wyłączeniu, na wniosek lub z urzędu, z postępowania kontrolnego, jeżeli wyniki kontroli mogłyby oddziaływać na jego prawa lub obowiązki, na prawa lub obowiązki jego małżonka albo osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnych i powinowatych do drugiego stopnia bądź osób związanych z nim z tytułu przysposobienia, opieki lub kurateli. Powody wyłączenia kontrolującego trwają także po ustaniu małżeństwa, przysposobienia, opieki lub kurateli.

2. Kontrolujący może być wyłączony, na wniosek lub z urzędu, z postępowania kontrolnego w każdym czasie, jeżeli zachodzą uzasadnione wątpliwości co do jego bezstronności.

3. O przyczynach powodujących wyłączenie kontrolujący lub kierownik jednostki kontrolowanej niezwłocznie zawiadamia Prezesa Urzędu.

4. O wyłączeniu kontrolującego postanawia Prezes Urzędu. Na postanowienie o wyłączeniu zażalenie nie przysługuje.

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

Art. 68.1. Upoważnienie do przeprowadzenia kontroli zawiera:

1) wskazanie podstawy prawnej przeprowadzenia kontroli;
2) oznaczenie organu kontroli;
3) imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli oraz numer jej legitymacji służbowej, a w przypadku osób, o których mowa w art. 66 ust. 2, imiona i nazwiska tych osób oraz numer paszportu lub innego dokumentu potwierdzającego tożsamość;
4) określenie zakresu przedmiotowego kontroli, w tym okresu objętego kontrolą;
5) oznaczenie podmiotu objętego kontrolą zwanego dalej „kontrolowanym”;
6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności kontrolnych;
7) podpis Prezesa Urzędu;
8) pouczenie podmiotu objętego kontrolą o jego prawach i obowiązkach;
9) datę i miejsce wystawienia imiennego upoważnienia.

2. W razie nieobecności kontrolowanego lub osoby przez niego upoważnionej, upoważnienie do przeprowadzenia kontroli oraz legitymacja służbowa lub inny dokument potwierdzający tożsamość mogą być okazane innemu pracownikowi kontrolowanego, który może być uznany za osobę, o której mowa w art. 97 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2017 r. poz. 459, 933 i 1132) lub przywołanemu świadkowi, którym powinien być funkcjonariusz publiczny, niebędący jednak pracownikiem organu przeprowadzającego kontrolę.

Art. 69.1. W celu uzyskania informacji mogących stanowić dowód w sprawie kontrolujący ma prawo:

1) wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń;
2) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli;

3) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego.

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 potwierdza je kontrolujący, o czym czyni wzmiankę w protokole kontroli.

4. W toku kontroli kontrolujący może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji. Organy kontroli państwowej lub Policja wykonują czynności na polecenie kontrolującego.

5. W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz. 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. 70.1. Kontrolujący może przesłuchać pracownika kontrolowanego w charakterze świadka.

2. Przed rozpoczęciem przesłuchania kontrolujący obowiązany jest uprzedzić świadka o odpowiedzialności karnej za zeznanie nieprawdy lub zatajenie prawdy, a w sytuacji określonej w ust. 3, informuje go o przysługujących mu uprawnieniach.

3. Osoba, o której mowa w ust. 1, może odmówić udzielenia informacji lub współdziałania w toku kontroli tylko wtedy, gdy naraziłoby to ją lub jej małżonka, wstępnych, zstępnych, rodzeństwo oraz powinowatych w tej samej linii lub stopniu, jak również osoby pozostające w stosunku przysposobienia, opieki lub kurateli, a także osobę pozostającą we wspólnym pożyciu, na odpowiedzialność karną. Prawo odmowy udzielenia informacji lub współdziałania w toku kontroli trwa po ustaniu małżeństwa lub rozwiązaniu stosunku przysposobienia, opieki lub kurateli.

Art. 71. Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Art. 72.1. Przebieg przeprowadzonej kontroli kontrolujący przedstawia w protokole kontroli.

2. Protokół kontroli powinien zawierać:

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 osób, o których mowa w art. 66 ust. 2, imię i nazwisko, numer paszportu albo innego dokumentu potwierdzającego tożsamość oraz numer upoważnienia;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu i zakresu 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) informację o pouczeniu 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 podpisują kontrolujący i kontrolowany.

4. Przed podpisaniem protokołu kontrolowany może, w terminie 7 dni od przedstawienia mu go do podpisu, złożyć pisemne zastrzeżenia do tego protokołu.

5. W razie zgłoszenia zastrzeżeń, o których mowa w ust. 4, 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 informuje o tym kontrolowanego na piśmie.

7. O odmowie podpisania protokołu kontrolujący czyni wzmiankę w protokole, zawierającą datę jej dokonania.

8. Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej doręcza się go kontrolowanemu.

Art. 73. Do kontroli działalności gospodarczej przedsiębiorcy, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2016 r. poz. 1829, 1948, 1997 i 2255 oraz z 2017 r. poz. 819), z wyłączeniem art. 79, art. 82 i art. 83.

Art. 74.1. Postępowanie kontrolne nie może trwać dłużej niż miesiąc od dnia podjęcia czynności kontrolnych. Za podjęcie czynności kontrolnych należy uznać moment, w którym kontrolujący okazuje kontrolowanemu, lub innej osobie wskazanej w przepisach, upoważnienie do przeprowadzenia kontroli oraz legitymację służbową lub inny dokument potwierdzający tożsamość.

2. Terminem zakończenia postępowania kontrolnego jest dzień podpisania protokołu kontrolnego przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 72 ust. 7.

3. W przypadku postępowania kontrolnego prowadzonego w toku postępowania administracyjnego terminu przewidzianego w ust. 1 nie wlicza się do terminów, o których mowa w art. 35 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego.

Art. 75. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli, Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania.

Art. 76. Na podstawie ustaleń kontroli Prezes Urzędu może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

Art. 77. W razie stwierdzenia, że działanie lub zaniechanie wyczerpuje znamiona przestępstwa określonego w ustawie, Prezes Urzędu kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Rozdział 8

Odpowiedzialność cywilna

Art. 78.1. Każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, może żądać, zaniechania tego działania a także może żądać ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków.

2. Wystąpienie z roszczeniem, o którym mowa w ust. 1, nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych.

3. W zakresie nieuregulowanym rozporządzeniem 2016/679 oraz niniejszą ustawą dochodzenie roszczeń, o których mowa w ust. 1, następuje na zasadach określonych przepisami Kodeksu cywilnego.

Art. 79.1. Do postępowania w sprawach roszczeń dochodzonych na podstawie art. 78, w zakresie nieuregulowanym niniejszą ustawą, stosuje się przepisy Kodeksu postępowania cywilnego.

2. Sąd okręgowy jest właściwy w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w tym roszczeń z tytułu art. 82 rozporządzenia 2016/679, niezależnie od wartości przedmiotu sporu.

Art. 80.1. O wniesieniu pozwu w sprawach, o których mowa w art. 78, sąd zawiadamia niezwłocznie Prezesa Urzędu.

2. Jeżeli przed Prezesem Urzędu albo sądem administracyjnym toczy się postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych albo postępowanie takie zostało zakończone, Prezes Urzędu zawiadamia o tym sąd, o którym mowa w ust. 1.

3. Sąd może zawiesić toczące się przed nim postępowanie do czasu zakończenia postępowania przed Prezesem Urzędu.

Art. 81. O każdym wyroku – uwzględniającym powództwo - w sprawach, o których mowa w art. 78 ust. 1 i 2, sąd zawiadamia Prezesa Urzędu.

Rozdział 9

Administracyjne kary pieniężne

Art. 82. Prezes Urzędu może nałożyć na podmioty nie będące organami publicznymi w rozumieniu w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego albo podmiotami publicznymi w rozumieniu w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, w drodze decyzji, administracyjne kary pieniężne na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

Art. 83.1. Na podmioty publiczne, o których mowa w art. 9 pkt 1 – 12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 zł.

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

Art. 84. 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. 85.1. Środki finansowe pochodzące z kar pieniężnych stanowią dochód budżetu państwa.

2. Karę pieniężną uiszcza się w terminie 14 dni od dnia upływu terminu na wniesienie skargi, albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego.

3. W razie upływu terminu, o którym mowa w ust. 2, kara pieniężna podlega ściągnięciu w trybie przepisów o postępowaniu egzekucyjnym w administracji.

Art. 86.1. Tworzy się Fundusz Ochrony Danych Osobowych, zwany dalej „Funduszem”, którego dysponentem jest Prezes Urzędu.

2. Fundusz jest państwowym funduszem celowym.

3. Przychodami Funduszu są środki finansowe pochodzące z 1% kar pieniężnych nakładanych przez Prezesa Urzędu. Środku z Funduszu nie mogą być podstawą osiągania przychodu przez pracowników Urzędu.

4. Wydatki Funduszu są przeznaczane na:

1) inicjowanie i podejmowanie przez Prezesa Urzędu przedsięwzięć w zakresie upowszechniania w społeczeństwie wiedzy o potrzebie ochrony danych osobowych oraz ryzyku, przepisach, zabezpieczeniach i prawach związanych z ich przetwarzaniem. Szczególną uwagę poświęca się działaniom skierowanym do dzieci;
2) inicjowanie i podejmowanie przez Prezesa Urzędu przedsięwzięć w zakresie upowszechniania wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych.

Art. 87.1. Prezes Urzędu może na wniosek podmiotu ukaranego odroczyć uiszczenie kary pieniężnej albo rozłożyć ją na raty ze względu na ważny interes wnioskodawcy.

2. Do wniosku dołącza się uzasadnienie.

3. W przypadku odroczenia uiszczenia kary pieniężnej albo rozłożenia jej na raty, Prezes Urzędu nalicza od nieuiszczonej kwoty odsetki w stosunku rocznym, których wysokość wynosi 50% stawki odsetek za zwłokę, ogłaszanej na podstawie art. 56 § 3 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.

4. W przypadku rozłożenia na raty kary pieniężnej, odsetki, o których mowa w ust. 3, są naliczane odrębnie dla każdej raty.

5. Odsetki są naliczane za okres od dnia upływu odroczonego terminu płatności kary pieniężnej albo terminu zapłaty poszczególnych rat.

6. Prezes Urzędu może uchylić odroczenie uiszczenia 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.

7. Rozstrzygnięcie Prezesa Urzędu w przedmiocie odroczenia uiszczenia kary pieniężnej albo rozłożenia jej na raty następuje w drodze postanowienia, na które nie przysługuje skarga do sądu administracyjnego.

Art. 88. Przepisów art. 189f i art.189k ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego nie stosuje się.

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 648, 768, 935, 1428 i 1537.

Rozdział 10

Przepisy karne

Art. 89.1. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie.

2. Orzekanie w sprawach o czyny określone w ust. 1 następuje w trybie przepisów ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia.

Art. 90.1. Kto bez podstawy prawnej przetwarza dane, o których mowa w art. 9 rozporządzenia 2016/679, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

2. Orzekanie w sprawach o czyny, o których mowa w ust.1, następuje w trybie przepisów ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. z 2016 r. poz. 1749 z późn. zm.[6])).

Rozdział 11

Przepisy końcowe

Art. 91.1. Maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy wynosi w roku:

1) 2018 r. - 27 214 000 zł;
2) 2019 r. - 16 298 000 zł;
3) 2020 r. - 16 509 000 zł;
4) 2021 r. – 16 285 000 zł;
5) 2022 r. – 16 515,000 zł;
6) 2023 r. - 16 285,000 zł;
7) 2024 r. – 16 516,000 zł;
8) 2025 r. - 16 285 000 zł;
9) 2026 r. – 16 515 000 zł;
10) 2027 r. – 18 015 000 zł.

[6)] Zmiany tekstu jednolitego wymienione ustawy zostały ogłoszone w Dz. U. z 2016 r. poz. 1948, 2138 i 2261 oraz z 2017 r. poz. 244, 773, 768 i 966.

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, a w przypadku IV kwartału - według stanu na dzień 20 listopada danego roku.

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 niniejszej ustawy.

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

Art. **92**. Ustawa wchodzi w życie w terminie i na zasadach określonych w ustawie z dnia …….. 2017 r. - Przepisy wprowadzające ustawę o ochronie danych osobowych (Dz. U. …….).

Za zgodność pod względem

prawnym, legislacyjnym i redakcyjnym

Katarzyna Prusak-Górniak

Dyrektor Departamentu Prawnego MC

/-podpisano elektronicznie/

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.

W **Rozdziale 1** wskazano zakres podmiotowy i przedmiotowy regulacji. Zgodnie z art. 1, ustawa będzie miała zastosowanie do ochrony osób fizycznych w związku z przetwarzaniem

ich danych osobowych. 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.” 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 kodeksie cywilnym (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.

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 zapewnienie 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.

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,

- działalności literackiej,

- działalności artystycznej,

- wypowiedzi akademickiej.

Rozporządzenie posługuje się terminem wypowiedzi akademickiej, artystycznej lub literackiej. Projektodawca zdecydował się na wprowadzenie terminu działalności literackiej i artystycznej, termin „wypowiedź" stosując wyłącznie względem aktywności akademickiej. Rozwiązanie podyktowane jest tym, że w ocenie projektodawcy termin „działalność" w kontekście aktywności literackiej i artystycznej jest tożsamy z terminem wypowiedź. Każda działalność artystyczna i literacka podejmowana jest bowiem, celem osiągnięcia rezultatu jakim jest wypowiedź artystyczna i literacka twórcy wyrażona w określonej formie. Jednocześnie termin „wypowiedź artystyczna" oraz „wypowiedź literacka" jest obcy polskiemu prawodawstwu. Odmiennie należy jednak ocenić określenie „wypowiedzi akademickiej", gdyż w ramach aktywności akademickiej sama wypowiedź stanowi tylko jeden z elementów działań podejmowanych przez uczelnie wyższe, które prowadzą zakrojoną na szeroką skalę działalność organizatorską, która nie zawsze może jednak zostać zakwalifikowana jako „wypowiedź akademicka".

Możliwość dokonania takich wyłączeń wynika z przepisu art. 85 Rozporządzenia. Zgodnie z tym przepisem państwa członkowskie przyjmują przepisy, pozwalające pogodzić prawo do ochrony danych osobowych na mocy Rozporządzenia z wolnością wypowiedzi i

informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej.

Dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej państwa członkowskie określają odstępstwa lub wyjątki od rozdziału II (Zasady), rozdziału III (Prawa osoby, której dane dotyczą), rozdziału IV (Administrator i podmiot przetwarzający), rozdziału V (Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych), rozdziału VI (Niezależne organy nadzorcze), rozdziału VII (Współpraca i spójność) oraz rozdziału IX (Szczególne sytuacje związane z przetwarzaniem danych), jeżeli są one niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji. Należy zwrócić uwagę, iż art. 85 Rozporządzenia stanowi samodzielną podstawę wyżej wymienionych wyłączeń bez potrzeby odwoływania się do treści art. 23 Rozporządzenia.

Proponowane brzmienie art. 2 projektu nowej ustawy o ochronie danych osobowych wskazuje relacje pomiędzy ochroną danych osobowych a działalnością dziennikarską, artystyczną, literacką i wypowiedzią akademicką. Przewidziane w nim wyłączenia stosowania przepisów Rozporządzenia uznano za niezbędne dla pogodzenia prawa do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji. Wyłączenia te mają pierwszeństwo, o ile korzystanie z nich nie narusza istotnie praw lub wolności podmiotu danych, np. poprzez wykorzystanie tych danych faktycznie w innym celu niż twórczość dziennikarska, artystyczna lub literacka (np. w celu zniesławienia).

W przypadku wszystkich ww. rodzajów wypowiedzi akademickiej wyłączono stosowanie art. 13,15 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),

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

- ograniczenia przetwarzania na wniosek osoby, której dane dotyczą (art. 18),

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

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

- prowadzenia 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 nie wymagającej 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. 3 projektu wdraża do polskiego porządku prawnego regulację art. 8 ust. 1 *in fine* Rozporządzenia. Zgodnie z treścią art. 8 ust. 1 Rozporządzenia:

„Jeżeli zastosowanie ma art. 6 ust. 1 lit. a, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat.”.

Art. 8 Rozporządzenia wyraża bezpośrednio skuteczną normę z wąsko określonym obszarem kompetencji państw członkowskich. Państwa członkowskie mają swobodę regulacyjną w określeniu granicy wieku dziecka, jeżeli zastosowanie ma art. 6 ust. 1 lit. a Rozporządzenia w przypadku usług społeczeństwa informacyjnego, oferowanych bezpośrednio dziecku. Państwa członkowskie mają w tym zakresie swobodę wyboru granicy wieku (tj.

granicy powyżej, której dziecko może samodzielnie wyrazić zgodę), ale wyłącznie w odniesieniu do osób, które ukończyły 13 lat. Należy podkreślić, iż jest to wyłącznie możliwość po stronie państw członkowskich, bez konieczności skorzystania z kompetencji regulacyjnej.

Co istotne, wskazana podstawa kompetencyjna dotyczy wyłącznie określenia granicy wieku dla skutecznego wyrażenia zgody przez dziecko i tylko w przypadku usług społeczeństwa informacyjnego, oferowanych bezpośrednio dziecku. Oznacza to w szczególności, iż art. 8 ust. 1 *in fine* Rozporządzenia nie przyznaje państwom członkowskim kompetencji do:

a) określenia ogólnej granicy wieku dla możliwości przetwarzania danych osobowych dziecka (niezależnie od podstawy legalizującej przetwarzanie danych osobowych);

b) modyfikacji zasad związania umową (art. 6 ust. 1 lit. b Rozporządzenia np. umowa o świadczenie usług drogą elektroniczną) jako podstawą przetwarzania danych (regulują to odrębne przepisy prawa umów państw członkowskich zgodnie z art. 8 ust. 3 Rozporządzenia);

c) określania mechanizmu wyrażania lub aprobowania zgody dziecka (tj. w jakiej sytuacji przedstawiciel ustawowy może zgodę wyrazić samodzielnie, a w jakiej wyłącznie potwierdza czynność dziecka);

d) regulacji sposobów weryfikacji tożsamości udzielających zgodę;

d) określania tego kto i w jakim trybie może zgodę wycofać;

e) regulacji problemu zgody – jako podstawy legalizującej przetwarzanie danych osobowych zgodnie - poza obszarem usług społeczeństwa informacyjnego (usług świadczonych drogą elektroniczną);

f) regulacji problemu zgody osoby ubezwłasnowolnionej.

Dodatkowo należy zwrócić uwagę, iż o ile art. 8 ust. 1 Rozporządzenia przesądza powyżej jakiej granicy wieku dziecko może samodzielnie udzielić zgody na przetwarzanie danych osobowych w ramach usług społeczeństwa informacyjnego, o tyle nie przesądza granicy wieku poniżej, której dziecko zgody w ogóle wyrazić nie może. Poniżej określonej granicy wieku (w przedziale 13-16 lat) w obrębie art. 8 ust. 1 Rozporządzenia, zgodę, o której mowa w art. 6 ust. 1 lit. a Rozporządzenia może wyrazić zarówno samodzielnie przedstawiciel ustawowy, jak i dziecko, jednak w tym drugim przypadku zgoda jest skuteczna po potwierdzeniu jej przez rodzica lub opiekuna prawnego.

W kontekście powyższego (niezależnie od oceny przedstawionej regulacji Rozporządzenia) należy wyraźnie podkreślić, iż przepisy Rozporządzenia (art. 8 ust. 1) nie przyznają państwom członkowskim kompetencji określenia granicy wieku, poniżej której dziecko w ogóle zgody - na przetwarzanie danych osobowych w zakresie usług społeczeństwa informacyjnego - wyrazić nie może. W tym zakresie w praktyce należy odwołać się przede wszystkich do ogólnych kryteriów skuteczności zgody wskazanych w art. 4 pkt 11, zgodnie z którym: „zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w formie oświadczenia lub wyraźnego działania, potwierdzającego, przyzwolenie na przetwarzanie dotyczących jej danych osobowych.

Projekt realizując kompetencję wskazaną w art. 8 ust. 1 *in fine* Rozporządzenia, obniża granicę wieku określoną w tym przepisie. Oznacza to, że zgodnie z projektem samodzielnie zgodę na przetwarzanie danych osobowych w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. zgodę na przetwarzanie danych osobowych w celu marketingu bezpośredniego administratora danych) będzie mogła wyrazić osoba, która ukończyła lat 13. Jednocześnie w celu zapewnienia pełnej efektywności regulacji art. 8 ust. 1 Rozporządzenia precyzuje, iż:

a) problem zgody dotyczy usług świadczonych drogą elektroniczną, oraz

b) wyrazić lub zaaprobować zgodę (wyrażoną przez dziecko, które nie ukończyło lat 13) może przedstawiciel ustawowy.

Ad. a)

Art. 8 ust. 1 Rozporządzenia posługuje się pojęciem usług społeczeństwa informacyjnego. Zgodnie natomiast z art. 4 pkt 25 Rozporządzenia, „usługa społeczeństwa informacyjnego" oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535. Biorąc pod uwagę treść art. 1 ust. 1 lit. b) Dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1), pojęcie „usługi społeczeństwa informacyjnego" należy traktować jako tożsame pojęciu: „usługi świadczonej drogą elektroniczną" zgodnie z treścią ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. W związku z tym w celu uniknięcia wątpliwości co do zakresu zastosowania art. 3 projektu, w tym zachowania systemowej zgodności, projekt w art. 3 posługuje się określeniem „usługi świadczonej drogą elektroniczną".

Ad. b)

Identyfikacja osoby uprawnionej do wyrażenia uprzedniej zgody (w oparciu o projektowany art. 3 ustawy) albo do potwierdzenia zgody wyrażonej przez osobę, która nie ukończyła lat 13 powinno następować przy uwzględnieniu treści przepisów ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny, dalej „k.c.", oraz ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy. W związku z tym projekt posługuje się ogólnym pojęciem przedstawiciela ustawowego.

Projektodawca zdecydował się skorzystać z kompetencji przyznanej mu na mocy art. 8 ust. 1 *in fine* Rozporządzenia. Można założyć, iż wskazana podstawa kompetencyjna ma na celu dostosowanie przepisów Rozporządzenia do ogólnych reguł skutecznego składania oświadczeń woli przez dzieci w systemach prawnych państw członkowskich, w tym w zakresie regulacji prawa prywatnego. Na marginesie należy zwrócić uwagę, iż przepisy o ochronie danych osobowych wprost odwołują się do prawa prywatnego w kontekście zgody na przetwarzanie danych osobowych. Motyw 42 Rozporządzenia, wskazuje, iż zgodnie z dyrektywą Rady 93/13/EWG (tj. w sprawie nieuczciwych warunków w umowach konsumenckich) oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem oraz nie powinno zawierać nieuczciwych warunków.

Należy zwrócić uwagę, iż w polskim systemie prawa cywilnego granicę wieku, kiedy małoletni może składać skuteczne (niekonieczne samodzielnie) oświadczenia woli, wyznacza ukończenie 13 lat. Zgodnie z art. 15 k.c. ograniczoną zdolność do czynności prawnych mają małoletni, którzy ukończyli lat trzynaście oraz osoby ubezwłasnowolnione częściowo. Ograniczona zdolność do czynności prawnych oznacza, iż małoletni może składać oświadczenia woli, z tym, że pewnych sytuacjach do ich skuteczności wymagana jest zgoda przedstawiciela ustawowego.

Przyjmując regulację kodeksu cywilnego jako „wzorzec regulacyjny" i możliwy punkt odniesienia przy ocenie adekwatnego wieku podejmowania świadomych decyzji przez małoletnich, należy wskazać, iż wyrażenie zgody na przetwarzanie danych osobowych stanowi jednocześnie oświadczenie woli w rozumieniu k.c.

W piśmiennictwie zauważono, iż w świetle regulacji k.c. zgoda na przetwarzanie danych osobowych nie podlega ograniczeniom wskazanym w art. 17 w zw. z art. 19 k.c. (nie jest to ani czynność prawna rozporządzająca ani zobowiązująca). Dlatego w świetle k.c.

skuteczną zgodę na przetwarzanie danych osobowych może samodzielnie wyrazić osoba, która ma co najmniej ograniczoną zdolność do czynności prawnych (przede wszystkim ukończyła lat 13 * – zob. szerzej M. Gumularz, „Charakter prawny oświadczenia w zakresie zgody na przetwarzanie danych", ABI Expert z 2017, nr 2). Zgoda osoby, która ukończyła 13 lat (i nie została ubezwłasnowolniona całkowicie) będzie legalizować ingerencję w dobro osobiste – dane osobowe – na gruncie art. 24 k.c.

W związku z powyższym z systemowego punktu widzenia istotne jest, aby ocena tego samego zachowania na gruncie różnych reżimów (ochrona danych osobowych oraz prawo cywilne) nie prowadziła do odmiennych wniosków co do skuteczności. Uzasadnia to przyjęcie granicy wieku 13 lat.

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. Przepis art. 4 projektu w celu zapewnienia stosowania art. 37 ust. 1 lit. a Rozporządzenia precyzuje, iż organami i podmiotami publicznymi obowiązanymi do wyznaczenia inspektora są organy publiczne wskazane w art. 5 par. 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, zwanego dalej „Kodeksem”, oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Na gruncie polskiego porządku prawnego odesłanie w zakresie pojęć „organ publiczny” i „podmiot publiczny”, do dwóch ww. ustaw, jako regulacji o podstawowym znaczeniu dla interpretacji ww. pojęć, wydaje się rozwiązaniem najbardziej racjonalnym i systemowo spójnym.

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, nie występujących 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 RODO. 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 2016/679 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 nowej ustawy 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.

Przepisy Rozporządzenia przewidują także, że administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora i zawiadamiają o nich organ nadzorczy.

Na tej podstawie prowadzona jest przez Prezesa Urzędu wewnętrzna ewidencja – przepisy Rozporządzenia nie wprowadzają obowiązku prowadzenia jawnego rejestru inspektorów. Natomiast obowiązek publikacji danych kontaktowych inspektora spoczywa zgodnie z art. 37 ust. 7 Rozporządzenia na administratorze oraz podmiocie przetwarzającym. Realizacji tego właśnie przepisu służy art. 5 projektu, regulujący sposób i tryb zawiadamiania o wyznaczeniu inspektora oraz prowadzenie ewidencji zawiadomień. Przewidując dużą liczbę zawiadomień, kierowanych w przyszłości do organu, przyjęto rozwiązanie, zgodnie z którym zawiadomienia należy przesyłać drogą elektroniczną. Co istotne, w zawiadomieniu należy wskazać adres poczty elektronicznej lub numer telefonu osoby wyznaczonej do pełnienia roli inspektora. Art. 5 projektu w sposób zamierzony nie przesądza, czy może to być adres e-mail ogólny (np. IOD@...) czy przypisany do konkretnej osoby (np. jan.kowalski@...). W praktyce należy dopuścić obie możliwości.

Na gruncie obowiązującej Ustawy podmiotem, który pełni podobną funkcję jak inspektor jest ABI. Powołanie ABI jest dobrowolne. Zadania ABI-ego określa art. 36a obowiązującej Ustawy.

Co istotne, przepisy Rozporządzenia nie przewidują możliwości wprowadzenia przez państwa członkowskie szczególnych regulacji w zakresie statusu i zadań inspektora.

Rozdział 3 projektu reguluje zasady certyfikacji i akredytacji oraz tryb postępowania w tych sprawach.

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.

W projekcie przewidziano, że certyfikacji dokonywał będzie wyłącznie Prezes Urzędu Ochrony Danych Osobowych, tym samym w projekcie nie było konieczne uregulowanie procedury akredytacji podmiotów certyfikujących. Zgodnie z art. 42 ust. 5 Rozporządzenia certyfikacji dokonują podmioty certyfikujące, o których mowa w art. 43 Rozporządzenia, lub dokonuje jej właściwy organ nadzorczy. Ustawodawca unijny przyznał więc państwom członkowskim swobodę w wyborze podmiotu który podejmował będzie działania certyfikacyjne. Zdecydowano o przyznaniu uprawnień do podejmowania działań certyfikacyjnych Prezesowi Urzędu Ochrony Danych Osobowych.

Jednocześnie należy wskazać, że w ocenie projektodawcy jednostka odpowiadająca za certyfikację wewnątrz struktury organizacyjnej Urzędu Ochrony Danych Osobowych nie powinna odpowiadać za prowadzenie postępowań w sprawie naruszenia przepisów o ochronie danych, w tym przeprowadzanie czynności kontrolnych. Ich powiązanie byłoby bowiem czynnikiem korupcjogennym lub generującym ryzyka braku obiektywizmu w przypadku kontroli. Podejmowaniu czynności certyfikacyjnych towarzyszyć powinna pełna bezstronność. Struktura organizacyjna organu nadzorczego powinna przyznawać temu pionowi pełną gwarancję bezstronności.

Przyznanie Prezesowi Urzędu wyłącznych kompetencji do podejmowania czynności certyfikacyjnych stanowi uzasadnienie do zwiększenia liczby zastępców organu. Bez wątpienia rekomendowanym rozwiązaniem byłoby przyznanie jednemu z nich kompetencji do wspierania Prezesa Urzędu w kierowaniu jednostką odpowiadającą za certyfikację w tym w zapewnieniu jej pełnej niezależności względem pozostałych jednostek jego struktury organizacyjnej.

Certyfikacji dokonuje się na wniosek administratora lub podmiotu przetwarzającego. Certyfikacji dokonuje się na podstawie kryteriów określonych przez Prezesa Urzędu i udostępnionych w BIP na jego stronie podmiotowej.

Postępowanie w sprawie udzielenia certyfikacji może zakończyć się czynnością materialno-techniczną jaką jest zawiadomienie wnioskodawcy o udzieleniu lub odmowie udzielenia certyfikacji. Natomiast odmowa udzielenia certyfikacja wiązała się będzie z obowiązkiem wydania decyzji administracyjnej. Wydając decyzję o odmowie udzielenia certyfikacji Prezes Urzędu obowiązany będzie wskazać kryteria, których nie spełnienie było powodem odmowy.

W przepisie art. 15 wskazano sytuacje kiedy cofa się certyfikację. Cofnięcie certyfikacji również następowało będzie w drodze decyzji administracyjnej. Certyfikacji udziela się na maksymalny okres 3 lat co wynika wprost z art. 42 ust. 7 Rozporządzenia. Przez cały ten okres administrator lub podmiot przetwarzający są obowiązani spełniać kryteria certyfikacji. W celu zapewnienia skutecznych narzędzi sprawdzania, czy kryteria certyfikacji są spełniane, przewidziano uprawnienie dla Prezesa Urzędu do przeprowadzania czynności sprawdzających. Zakres uprawnień przysługujących w ramach prowadzenia czynności sprawdzających określa art. 14 projektu. Dokumentem potwierdzającym certyfikację jest certyfikat.

Przepisy art. 17-19 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.

Rozdział 4 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 celem wydania aktu zapewniającego skuteczne stosowanie Rozporządzenia a obecna 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, o tyle podstawą działań podejmowanych przez społecznych inspektorów pracy jest ustawa z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy. 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 inspektów 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.

Nowy organ ochrony danych osobowych będzie miał znacznie szerszy zakres uprawnień niż dzisiejszy GIODO. Będzie on nie tylko organem nadzorczym w rozumieniu Rozporządzenia ze znacznie szerszym zakresem uprawnień i obowiązków niż dzisiejszy GIODO, ale będzie również organem nadzorczym 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 uchylająca decyzję ramową Rady 2008/977/WSiSW. Projekt przepisów Rozporządzenia przewiduje również procedurę powołania Prezesa Urzędu. Ma być on powołany przez Sejm za zgodą Senatu na wniosek Prezesa Rady Ministrów. Rozporządzenie w art. 53 stanowi, iż państwa członkowskie zapewniają, by każdy członek ich organów nadzorczych był powoływany w drodze przejrzystej procedury przez:

- ich parlament,
- ich rząd,
- ich głowę państwa, lub
- niezależny organ uprawniony do powoływania członków organu nadzorczego na podstawie prawa państwa członkowskiego.

Odnosząc się do ww. gwarancji niezależności nowego Prezesa Urzędu przyznawanych na etapie jego powołania uznano, że utrzymanie dotychczasowych rozwiązań w tym zakresie tj. tryb powoływania przez Sejm na wniosek Prezesa Rady Ministrów oraz przyznanie Prezesowi Urzędu immunitetu, analogicznie jak dotychczasowemu Generalnemu Inspektorowi Ochrony Danych Osobowych, będzie najlepszą gwarancją niezależności tego organu. Włączenie Prezesa

Rady Ministrów w procedurę powołania Prezesa Urzędu uzasadnione jest pozycją ustrojową Prezesa Urzędu, który w trakcie swoich działań współpracuje zarówno w władzą ustawodawczą jak i wykonawczą, uczestnicząc w procedurze tworzenia prawa i sprawując nadzór nad przetwarzaniem danych osobowych we wszystkich obszarach działania państwa. W związku z powyższym, powołaniu na piastuna organu najlepszego kandydata towarzyszyć powinno pełne porozumienie pomiędzy zarówno władzą ustawodawczą jak i wykonawczą, przy przyznaniu jednak organowi wszelkich atrybutów jego niezależności – w tym jego podległość w zakresie wykonywanych zadań wyłącznie ustawie.

Regulację w zakresie warunków, jakie musi spełniać kandydat na Prezesa Urzędu określa art. 20 ust. 4 projektu. Projekt ustawy zawiera regulacje dotyczące zakazu członkostwa Prezesa Urzędu w partii politycznej, związku zawodowym, zakazu zajmowania innego stanowiska, z wyjątkiem stanowiska naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, wykonywania innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu oraz zakazu prowadzenia działalności publicznej niedającej się pogodzić z godnością jego urzędu. Do warunków których spełnienie stanowi wymóg objęcia stanowiska Prezesa Urzędu należy w szczególności pięcioletnie doświadczenie w wykonywaniu czynności bezpośrednio związanych z ochroną danych osobowych oraz posiadanie stopnia naukowego doktora. Spełnienie powyższych warunków w ocenie projektodawcy stanowi gwarancję objęcia stanowiska Prezesa Urzędu przez specjalistę posiadającego zarówno rozbudowaną teoretyczną jak i praktyczną wiedzę w obszarze ochrony danych osobowych. Projektodawca wprowadzając wymóg posiadania stopnia doktora jako warunkujący pełnienie funkcji Prezesa Urzędu umocowuje godną pełnego poparcia i wykształconą od lat w Polsce praktykę powoływania na piastuna organu jakim jest Generalny Inspektor Ochrony Danych Osobowych osób posiadających taki stopień naukowy. Powyższe wpisuje się również w edukacyjną rolę organu nadzorczego jakim jest Generalny Inspektor Ochrony Danych Osobowych i jakim będzie Prezes Urzędu. Przy podejmowaniu decyzji w powyższym zakresie, projektodawca uwzględnił również kwalifikacje posiadane przez dotychczasowych piastunów organu jakim jest Generalny Inspektor Ochrony Danych Osobowych. Niemal każdy z nich posiadał stopień naukowy doktora nauk. Wskazane powyżej wymogi stanowią w ocenie projektodawcy dodatkową gwarancję niezależności organu poprzez podkreślenie jego apolitycznej i eksperckiej pozycji w ramach ustroju organów państwowych. W porównaniu z warunkami zawartymi w art. 8 ust. 3 obowiązującej Ustawy zrezygnowano z warunku stałego

zamieszkiwania na terytorium Rzeczypospolitej Polskiej, jako nieuzasadnionego i trudnego do weryfikacji, zrezygnowano także z warunku dotyczącego wyróżniania się wysokim autorytetem moralnym jako trudno mierzalnego. W ocenie projektodawcy kryteria warunkujące możliwość pełnienia specjalistach kierowniczych funkcji państwowych powinny podlegać łatwej weryfikacji i mieć charakter formalny. Zmieniono również kryterium wykształcenia warunkującego możliwość ubiegania się o stanowisko Prezesa Urzędu. Piastun organu nie musi być bowiem prawnikiem, może być tytułem przykładu specjalistą w obszarze sektora IT bliskiego ochronie danych osobowych, posiadając jednak wiedzę z zakresu ochrony danych osobowych. Dodano wymóg korzystania z pełni praw publicznych oraz doprecyzowano wymóg niekaralności.

Projektowana ustawa przewiduje wprost, iż odwołanie Prezesa następuje w przypadku gdy Prezes zrzekł się stanowiska, stał się trwale niezdolny do pełnienia obowiązków na skutek choroby, został skazany prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego albo sprzeniewierzył się ślubowaniu. Nie przewidziano więc zmian w zakresie przesłanek odwołania. Szczególne wątpliwości w tym zakresie budzi art. 53 ust. 4 Rozporządzenia, w świetle którego *członek może zostać odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki niezbędne do pełnienia obowiązków*. Poważne uchybienie może stanowić zarówno rażące naruszenie prawa w związku z przewlekłością postępowania, jak i skazanie prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa. Uwzględniając jednak konieczność zapewnienia pełnej niezależności Prezesowi Urzędu, projektodawca odstąpił od wprowadzania do projektu przesłanki rażącego naruszenia prawa jako podstawy do odwołania Prezesa Urzędu uznając, że jest nią skazanie prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa w tym przestępstwa skarbowego.

Gwarancją niezależności Prezesa Urzędu jest również przyznanie mu kompetencji do samodzielnego nadawania statutu. Novum przy regulacjach dotyczących tej jednostki jest nadawanie jej statutu przez Prezesa Urzędu, a nie jak jest w przypadku Generalnego Inspektoratu Ochrony Danych Osobowych przez Prezydenta RP. Organ sam decydował będzie więc o strukturze organizacyjnej Urzędu oraz zadaniach realizowanych przez jego zastępców oraz pracowników Urzędu. Nowością są również regulacje dotyczące obowiązku zachowania tajemnicy przez pracowników Urzędu. Powyższa regulacja ma za zadanie zapewnienie stosowania art. 54 ust. 2 Rozporządzenia.

Gwarancją niezależności organu jest również jego niezależność budżetowa.

Podobnie jak dzisiaj w przypadku GIODO, kadencja Prezesa Urzędu będzie trwała 4 lata i ta sama osoba nie będzie mogła być Prezesem Urzędu dłużej niż przez dwie kadencje.

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. Ze względu na wykonywanie przez Prezesa Urzędu zadań organu nadzorczego 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 uchylająca decyzję ramową Rady 2008/977/WSiSW, przewidziano w projekcie, iż jednego zastępcę Prezesa będzie powoływał Prezes Rady Ministrów na wniosek ministra właściwego do spraw wewnętrznych. Wniosek taki minister właściwy do spraw wewnętrznych będzie obowiązany przekazać celem zaopiniowania Ministrowi Sprawiedliwości, Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw finansów publicznych oraz Prokuratorowi Generalnemu.

Pozostali zastępcy powoływani będą na wniosek ministra właściwego do spraw informatyzacji. Uzasadnieniem do powoływania dwóch zastępców na wniosek właśnie ministra właściwego do spraw informatyzacji jest fakt, iż zgodnie z 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.) do zakresu działania ministra właściwego do spraw informatyzacji należą sprawy kształtowania polityki państwa w zakresie ochrony danych osobowych .

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 (art. 34 ust. 7). Ideą jest by różne podmioty mogły wesprzeć swoją wiedzą Prezesa Urzędu. Zadania ww. Rady określa art. 34 ust. 2 projektu.

Przepis art. 35 projektu stanowi o sprawozdaniach składanych przez Prezesa Urzędu i służy zapewnieniu stosowania art. 59 Rozporządzenia.

Przepis art. 36 projektu 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.

Regulacja zawarta w art. 37 projektu stanowi 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. Przepis art. 38 projektu dotyczy udostępniania przez Prezesa Urzędu w Biuletynie Informacji Publicznej standardowych klauzul umownych i zatwierdzonych kodeksów postępowania i służy wskazaniu sposobu podawania do publicznej wiadomości ww. dokumentów.

Uregulowanie zawarte w art. 39 projektu 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.

Celem art. 40 jest zapewnienie sprawności i zakończenia w rozsądnym czasie postępowania dotyczącego uprzednich konsultacji, o których mowa w art. 36 Rozporządzenia. Przepis ust. 2 art. 36 Rozporządzenia daje organowi nadzorczemu (Prezesowi Urzędu) termin 8 tygodni na przedstawienie zaleceń i ewentualnie skorzystanie z uprawnień przewidzianych w art. 58

Rozporządzenia. Termin ten może być wydłużony o 6 tygodni. Wreszcie bieg tych terminów można zawiesić do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji. W opinii projektodawcy nie wskazanie terminu zawieszenia postępowania może doprowadzić, w skrajnym przypadku, do sytuacji gdy zalecenia nigdy nie zostaną wydane a administrator nie będzie mógł przystąpić do przetwarzania danych. Celem tego przepisu jest zatem zapewnienie administratorom prawa do rozpatrzenia ich sprawy przez Prezesa Urzędu w rozsądnym terminie. W ocenie projektodawcy maksymalny termin 16 tygodni jest wystarczający na sformułowanie zaleceń i ewentualnie skorzystanie z uprawnień przewidzianych w art. 58 Rozporządzenia.

Celem przepisu art. 42 jest określenie, iż dla czynności w nim wymienionych przyjmuje się formę decyzji administracyjnej. Wprowadzenie tej formy rozstrzygnięcia Prezesa Urzędu ma na celu zapewnienie odpowiedniego poziomu ochrony stron postepowania. Przy wydawaniu tych decyzji zastosowanie będą miały przepisy o postępowaniu zawarte w Rozdziale 5 projektu, z wyłączeniem art. 53 dotyczącego wydawania postanowień dotyczących ograniczenia przetwarzania danych osobowych i art. 55 dotyczącego rodzaju rozstrzygnięć wydawanych w toku postepowania. Wyłączenie wynika z tego, iż ww. przepisy nie znajdą zastosowania w sprawach wymienionych w art. 42.

Przepisy art. 43 projektu 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. przepis 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 dopasowywane 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 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.

Przepisy **Rozdziału 5** 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 postepowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej. Zasada stosowania w sprawach nieuregulowanych Kodeksu postepowania administracyjnego 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 Kodeksie. Wyłączenie stosowania Kodeksu i próba stworzenia szczególnego postępowania w sprawie naruszenia przepisów o ochronie danych obarczona byłaby z jednej strony ryzykiem nie uregulowania niezbędnych elementów postępowania a z drugiej koniecznością tworzenia obszernej listy przepisów Kodeksu, które jednak znalazłyby zastosowanie w postępowaniu. Działania takie uznano za nieracjonalne.

Postępowanie będzie prowadzone przez Prezesa Urzędu jako organ właściwy w sprawie ochrony danych osobowych. Korzystając z możliwości przewidzianej w Konstytucji RP oraz w Kodeksie 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.

Obok jednoinstancyjności kolejną odrębnością postępowania przewidzianego w ustawie w stosunku do postępowania unormowanego w Kodeksie jest rozszerzenie prawa organizacji

społecznych do wystąpienia z żądaniem wszczęcia postępowania albo dopuszczenia ich do udziału w postępowaniu. Na gruncie art. 31 Kodeksu organizacja społeczna może w sprawie dotyczącej innej osoby występować z żądaniem: 1) wszczęcia postępowania, 2) dopuszczenia jej do udziału w postępowaniu, jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes społeczny. Przepisy projektowanej ustawy umożliwiają udział organizacji społecznej w postępowaniu także wówczas, gdy organizacja nie może wykazać się istnieniem interesu społecznego w danej sprawie. W sprawach o naruszenie praw przysługujących na mocy przepisów o ochronie danych osobowych wystarczy, jeśli organizacja społeczna uzasadni swój udział w postępowaniu tym, że za jej udziałem przemawia interes osoby, której prawa zostały naruszone. Dodatkową przesłanką udziału organizacji społecznej w postępowaniu, zarówno na gruncie Kodeksu jak i projektowanej ustawy jest istnienie uzasadnienia tego udziału z punktu widzenia celów statutowych organizacji. Powyższa regulacja ma na celu zapewnienie stosowania art. 80 Rozporządzenia.

Kolejny przepis projektowanej ustawy (art. 46) wskazuje, iż organ zawiadamiając strony o każdym przypadku niezałatwienia sprawy w terminie oprócz, jak dotychczas, podania przyczyn zwłoki i nowego terminu załatwienia sprawy jest obowiązany podać także informację o stanie sprawy i przeprowadzonych w jej toku czynnościach. Regulacja ta stanowi modyfikację art. 36 Kodeksu i służy zapewnieniu 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 56 Rozporządzenia nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 77 do organu nadzorczego. Przyjmując, iż zgodnie z Kodeksem 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 regulacja art. 46 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.

Celem przepisu art. 47 projektu jest jak najpełniejsza realizacja wyrażonej w Kodeksie zasady prawdy obiektywnej, obowiązku wszechstronnego wyjaśnienia okoliczności sprawy oraz zapewnienia sprawności postępowania. Przepis ten pozwala Prezesowi Urzędu wyznaczyć

stronie termin na przedstawienie dowodu będącego w jej posiadaniu oraz żądać od strony tłumaczenia dokumentacji sporządzonej w języku obcym. Przepis ten pozwoli również sądom administracyjnym badającym legalność postępowania prowadzonego przez Prezesa Urzędu stwierdzić, czy organ wykorzystał wszelkie przewidziane prawem możliwości w celu wszechstronnego wyjaśnienia danej sprawy.

Projektowany przepis art. 48 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.

Kolejne przepisy projektu odnoszą się 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 2003 r. poz. 1503, z późn. zm.). 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.

Odnosząc się do ograniczenia prawa wglądu do materiału dowodowego (art. 50) 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 art. 51 projektu stanowi modyfikację przepisu art. 88 Kodeksu. Celem tego przepisu jest zwiększenie z 50 zł do 500 zł wysokości grzywny za nie stawienie 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 waga spraw związanych z naruszeniem przepisów o ochronie danych osobowych wymaga zapewnienia sprawności i skuteczności postępowań w tych sprawach. Dolegliwa kara grzywny jest instrumentem temu służącym.

Przepis art. 53 projektu ma 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. Nie zdecydowano o wprowadzeniu do przepisów projektu ustawy instytucji zażalenia na to postanowienie. Postanowienie to jest natomiast zaskarżalne w skardze na decyzję kończącą postępowanie w sprawie. Decyzja ta, zgodnie z art. 35 Kodeksu, powinna zostać wydana niezwłocznie, w sprawie wymagającej postępowania wyjaśniającego nie później niż w ciągu miesiąca, a w sprawie szczególnie skomplikowanej - nie później niż w ciągu dwóch miesięcy od dnia wszczęcia postępowania. Powyższe oznacza, że w przypadku wprowadzenia zażalenia na ww. postanowienie, które musiałoby również zostać przekazane do sądu administracyjnego i przez ten sąd rozpatrzone, czynności związane z rozpatrzeniem tego zażalenie mogłyby zbiec się w czasie z wniesieniem i rozpatrywaniem skargi na decyzję Prezesa Urzędu a w skrajnym przypadku trwać nawet dłużej. Obowiązujące przepisy o postępowaniu sądowoadministracyjnym nie regulują takich sytuacji ani nie rozstrzygają jak powinien zachować się wówczas sąd. Jednocześnie nie budzi wątpliwości, że ww. postanowienie nie może obowiązywać dłużej niż do czasu wydania decyzji kończącej postępowanie w sprawie (art. 53 ust. 2 projektu). Tym samym w ocenie projektodawcy dla zapewnienia spójności obowiązujących regulacji zasadnym jest przyjęte rozwiązanie, iż postanowienie zobowiązujące podmiot do ograniczenia przetwarzania danych osobowych jest zaskarżalne w skardze na decyzję Prezesa Urzędu.

W projekcie ustawy – w zakresie rozstrzygnięć jakie mogą zapaść po przeprowadzeniu postępowania odesłano do art. 58 ust. 2 lit. b-j rozporządzenia 2016/679. Uznano za niecelowe przepisywanie przepisów Rozporządzenia w tym zakresie. Nowym elementem, a jednocześnie modyfikacją przepisów Kodeksu, 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.

Przepis art. 56 projektu ustawy pozwala, w przypadku znikomej wagi naruszenia oraz jego zaprzestania przez stronę, udzielić stronie, w drodze decyzji administracyjnej, upomnienia. Przepis ten ma na celu zapewnienie stosowania art. 58 ust. 2 lit. b Rozporządzenia, który stanowi o uprawnieniu organu nadzorczego do udzielania upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów Rozporządzenia przez operacje przetwarzania danych. W Kodeksie przepis art. 189f § 1 stanowi, że organ administracji publicznej, w drodze decyzji, odstępuje od nałożenia administracyjnej kary pieniężnej i poprzestaje na pouczeniu m.in. jeżeli waga naruszenia prawa jest znikoma, a strona zaprzestała naruszania prawa. W projekcie ustawy zdecydowano się wprowadzić pojęcie upomnienia. W odróżnieniu od Kodeksowego pouczenia upomnienie może być stosowane „obok" administracyjnej kary pieniężnej. Postanowiono jednak przyjąć dla upomnienia takie same przesłanki jak dla Kodeksowego pouczenia.

Przepis art. 57 projektu jest związany z przepisem art. 83 projektu. Przepis art. 57 nakłada na Prezesa Urzędu obowiązek ogłaszania w Biuletynie Informacji Publicznej prawomocnych decyzji administracyjnych zawierających rozstrzygnięcia, o których mowa w art. 58 ust. 2 lit. b – g i lit. j Rozporządzenia, wydanych wobec organów, o których mowa w art. 5 § 2 pkt 3 Kodeksu postępowania administracyjnego albo podmiotów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, zwanych dalej łącznie „podmiotami publicznymi". Podmioty publiczne mają natomiast obowiązek udostępniania na swoich stronach internetowych informacji o działaniach podjętych w celu wykonania ww. 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 przepisie art. 84 projektu ograniczono wysokość administracyjnej kary pieniężnej, którą można nałożyć na podmioty publiczne do 100 000 zł.

Przepis art. 58 stanowi powielenie przepisów obowiązującej ustawy (art. 18 ust. 2a).

Odnosząc się do art. 59 projektu wskazać należy, że decyzje wydane przez Prezesa Urzędu w postepowaniu jednoinstancyjnym są decyzjami ostatecznymi podlegają więc natychmiastowemu wykonaniu. Zgodnie z art. 61 § 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi wniesienie skargi nie wstrzymuje wykonania

aktu lub czynności. Wyjątek od tej zasady wprowadza art. 59 ust. 2 projektu, który stanowi, że wniesienie przez stronę skargi do sądu administracyjnego powoduje wstrzymanie wykonania decyzji w zakresie dotyczącym administracyjnej kary pieniężnej. Przyjęto ustawowe wstrzymanie wykonalności decyzji administracyjnej nakładającej administracyjną karę pieniężną, tak by dopiero po rozpatrzeniu sprawy przez sąd i oddaleniu skargi decyzja taka podlegała wykonaniu. Wynika to oczywiście z dolegliwości administracyjnej kary pieniężnej.

W projekcie ustawy nie przewiduje się zażaleń na postanowienia jako odrębnych środków odwoławczych. Wszystkie postanowienia wydawane w toku postępowania będą podlegały zaskarżeniu w skardze na decyzję Prezesa Urzędu. Zapewni to rozpatrzenie w jednym postępowaniu sadowoadministracyjnym wszystkich spraw związanych z prowadzonym przez Prezesa Urzędu postępowaniem.

Wreszcie ostatnie wyłączenie w odniesieniu do Kodeksu dotyczy przepisu art. 66a Kodeksu. Przepis art. 66a Kodeksu reguluje kwestię zakładania metryki sprawy. Projektodawca uznał, że obowiązek jej prowadzenia w formie wskazanej w Kodeksie można wyłączyć przy założeniu prowadzenia przez Prezesa Urzędu elektronicznego systemu zarządzania dokumentacją, w którym dokumentowane są wszystkie czynności dokonywane w sprawie i osoby ich dokonujące.

Przepisy **Rozdziału 6** 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, 62 ust. 7 oraz 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. Po drugie należy wskazać, że rozwiązanie wprowadzone do projektu ustawy o ochronie danych osobowych nie jest 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. Po trzecie, 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. Obawy budzi również brak przewidzenia wprost w projekcie środków zaskarżenia na wydawane przez Prezesa Urzędu postanowienie. Organem właściwym do rozpatrzenia takiego środka powinien być sąd, uwzględniając jednak krótkie wynikające z Kodeksu terminy do rozstrzygnięcia sprawy przez Prezesa Urzędu, rozstrzygnięcie sądu mogłoby nastąpić później, niż wydanie rozstrzygnięcia przez Prezesa Urzędu. Nie oznacza to, że przedsiębiorca nie będzie mógł odwołać się od treści środka tymczasowego. Będzie mógł zrobić to w odwołaniu od decyzji wydanej przez Prezesa Urzędu, a wyrok sądu administracyjnego będzie podstawą do ewentualnego dochodzenia odpowiedzialności odszkodowawczej na drodze cywilnej. Przewidziane rozwiązanie, jest również odpowiedzią na sygnalizowaną potrzebę nieraz natychmiastowej reakcji na naruszenie ochrony danych osobowych, gdzie skutki naruszenia odczuwalne są dla obywatela bardzo często każdego dnia, i każdy dzień trwania postępowania przez Prezesa Urzędu wiąże się z poważnymi skutkami.

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 by 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. Uwzględniając, że krajowe przepisy o ochronie danych osobowych nie mogą nakładać jakichkolwiek obowiązków na inne państwa członkowskie, art. 64 ust. 2 nakłada na Prezesa Urzędu obowiązek tłumaczenia na język polski wszelkiej formalnej korespondencji doręczanej do niego w ramach mechanizmów współpracy w innym języku, o ile w związku z podejmowanymi czynnościami mogą mieć one jakikolwiek wpływ na sytuację prawną jakiejkolwiek osoby bądź podmiotu. Powyższy przepis dotyczył będzie w szczególności korespondencji doręczanej Prezesowi Urzędu w związku z podejmowanymi przez niego czynnościami kontrolnymi bądź prowadzonym postępowaniem.

Dokonywanie efektywnej współpracy wymaga dokładnego doprecyzowania zakresu zadań podejmowanych przez każdy z organów nadzorczych państw członkowskich. Art. 64 ust. 1 projektu ustawy nakłada wymóg przyjęcia przez Prezesa Urzędu podejmującego wspólne operacje, o których mowa w art. 62 ust. 1 Rozporządzenia, z innymi organami nadzorczymi państw członkowskich wykaz ustaleń dotyczących takich wspólnych operacji. Krajowe przepisy o ochronie danych osobowych nie mogą nakładać obowiązku podejmowania takich działań przez inne państwa członkowskie, adresatem obowiązku jest więc Prezes Urzędu. Rozwiązanie takie nie jest obce polskim przepisom prawnym, i wprowadzone zostało również do art. 5 ust. 1 ustawy z dnia 7 lutego 2014 r. o udziale zagranicznych funkcjonariuszy lub

pracowników we wspólnych operacjach lub wspólnych działaniach ratowniczych na terytorium Rzeczypospolitej Polskiej.

W przepisach **Rozdziału 7** 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. Zakres udzielanych upoważnień do przeprowadzenia kontroli określa art. 68 projektu. Do przeprowadzania kontroli będą również uprawnieni członkowie lub pracownicy organu nadzorczego innego państwa członkowskiego. 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.

Dla zapewnienia możliwości przeprowadzenia kontroli pod nieobecność kontrolowanego przewidziano, w art. 68 ust. 2, że upoważnienie do przeprowadzenia kontroli będzie mogło być okazane pracownikowi kontrolowanego lub przywołanemu świadkowi, którym powinien być funkcjonariusz publiczny.

Zakres uprawnień kontrolujących oraz obowiązków kontrolowanych określa art. 69 projektu. Porównując projektowaną regulację do regulacji art. 14 obowiązującej Ustawy należy zauważyć, iż zrezygnowano z ograniczenia czasu przeprowadzania kontroli do godzin 6.00 – 22.00, uznając, iż ochrona danych osobowych może w pewnych sytuacjach wymagać podjęcia nagłych czynności kontrolnych. Postanowiono zatem nie wyłączać z mocy ustawy możliwości przeprowadzenia kontroli poza ww. godzinami.

Ważną i nową regulacją, mająca na celu skuteczne przeprowadzenie czynności kontrolnych, jest przepis art. 69 ust. 4 pozwalający kontrolującym korzystać z pomocy funkcjonariuszy innych organów kontroli lub Policji.

Przebieg przeprowadzonej kontroli kontrolujący przedstawi w protokole kontroli. Zawartość tego protokołu określa art. 72 ust. 2 projektu. Zasadą jest, iż protokół podpisują kontrolujący i kontrolowany. W przypadku odmowy podpisania protokołu przez kontrolowanego, kontrolujący czyni o tym wzmiankę w protokole.

Przepis art. 73 projektu przewiduje stosowanie do postępowania kontrolnego w przypadku kontroli działalności gospodarczej przedsiębiorcy przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, z wyjątkiem przepisów art. 79, 82 i 83. Powyższe oznacza, że nie będą miały zastosowania do kontroli przestrzegania przepisów o ochronie danych osobowych przepisy dotyczące zawiadomienia o zamiarze wszczęcia kontroli, zakazu podejmowania i prowadzenia więcej niż jednej kontroli działalności przedsiębiorcy oraz ograniczeń w zakresie czasu trwania wszystkich kontroli organu kontroli u przedsiębiorcy w jednym roku kalendarzowym. W opinii projektodawcy zastosowanie ww. przepisów mogłoby uniemożliwić rzetelne i przeprowadzone we właściwym czasie postępowanie kontrolne w zakresie przestrzegania przepisów o ochronie danych osobowych. Trudno bowiem sobie wyobrazić, że kontrola doraźna w ww. zakresie nie mogłaby się odbyć z uwagi np. na trwającą kontrolę przestrzegania przepisów z zakresu ochrony środowiska. Ochrona prawa podstawowego jakim jest prawo do ochrony danych osobowych mogłaby wówczas stać się iluzją.

Nową i ważną regulacją, mając na uwadze obecną praktykę, jest przepis art. 74 projektu, który przewiduje, że postępowanie kontrolne nie może trwać dłużej niż miesiąc od dnia podjęcia czynności kontrolnych. Przy czym za podjęcie czynności kontrolnych należy uznać moment, w którym kontrolujący okazuje kontrolowanemu, lub innej osobie wskazanej w przepisach, upoważnienie do przeprowadzenia kontroli oraz legitymację służbową lub inny dokument potwierdzający tożsamość. Celem tego przepisu jest ograniczenie w czasie czynności kontrolnych prowadzonych przez organ, tak by dla podmiotów kontrolowanych nie istniała uciążliwość oraz niepewność związana z długotrwałym prowadzeniem tego postępowania. Co ważne za dzień zakończenia postępowania kontrolnego przyjęto dzień podpisania protokołu przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 72 ust. 7.

Kolejną nową w porównaniu z obowiązującą Ustawą i ważną regulacją jest przepis art. 74 ust. 3 projektu. Stanowi on, że czasu trwania postępowania kontrolnego nie wlicza się do terminów załatwiania spraw przewidzianych w art. 35 Kodeksu. Powyższe oznacza, że w przypadku prowadzenia przez organ w ramach postępowania czynności kontrolnych, to termin załatwienia sprawy przewidziany w art. 35 Kodeksu może się wydłużyć maksymalnie o miesiąc. Celem regulacji jest zapewnienie Prezesowi Urzędu właściwego czasu na rzetelne przeprowadzenie i udokumentowanie czynności kontrolnych oraz wszechstronne zbadanie i rozpatrzenie okoliczności sprawy. Powyższe nabiera szczególnego znaczenia w kontekście art. 83

Rozporządzenia, który przewiduje możliwość nałożenia na administratorów lub podmioty przetwarzające wysokich administracyjnych kar pieniężnych.

Rozdział 8 (art. 78-81) projektu ustawy odnosi się do odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych.

Art. 78 projektu 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

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 projektowany art. 78 nie dotyczy roszczeń odszkodowawczych, które mogą być realizowane w przypadku poniesienia szkody majątkowej lub niemajątkowej w wyniku naruszenia przepisów Rozporządzenia w oparciu o art. 82 Rozporządzenia.

Art. 78 ust. 2 projektu wyraźnie przesądza, iż dochodzenie roszczeń w oparciu o art. 78 projektu nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych. Celem tej regulacji jest m.in. rozstrzygnięcie ewentualnych wątpliwości, które mogłyby dotyczy relacji pomiędzy art. 78 projektu oraz art. 82 Rozporządzenia.

W doktrynie i orzecznictwie, nie budzi wątpliwości, iż naruszenie danych osobowych stanowi jednocześnie naruszenie dóbr osobistych. Art. 23 k.c. zawiera otwarty katalog dóbr osobistych. Natomiast dane osobowe ujmowane są jako kategoria dobra osobistego - prywatności. Dane osobowe nie mają więc charakteru samoistnego dobra osobistego (tak P. Sobolewski, Kodeks cywilny. Komentarz. Tom I. Przepisy wprowadzające. Część ogólna. Własność i inne prawa rzeczowe, K. Osajda (red.), Warszawa jako: „sfera fizycznej przestrzeni, a także myśli i przeżyć człowieka oraz informacji o nim, do której dostęp można uzyskać tylko za jego zgodą (przy czym zakres ochrony tej sfery może być różny ze względu na pełnioną przez daną osobę rolę społeczną)" (P. Machnikowski, Kodeks cywilny. Komentarz, E. Gniewek, P. Machnikowski (red.), Warszawa 2016, komentarz do art. 23 k.c., teza 2). Jednocześnie w piśmiennictwie podkreśla się, iż „Prywatność jest pojęciem wieloznacznym, trudnym do zdefiniowania. W wyjaśnieniach doktryny dotyczących istoty prywatności zwraca się zwłaszcza uwagę na aspekt poszanowania prawa człowieka do odosobnienia się, pozostawienia w spokoju, co przekłada się na ujęcie prywatności jako obszaru niedostępności, wolnego od ingerencji zewnętrznej, stwarzającego warunki do swobodnego kształtowania własnego życia i rozwoju własnej osobowości. Wskazuje się również, w nawiązaniu do przepisów konstytucyjnych, że za istotny komponent prywatności należy uznać autonomię człowieka w decydowaniu o swoim życiu osobistym (art. 47 Konstytucji RP), a także autonomię informacyjną" (Panowicz-Lipska, Kodeks cywilny. Komentarz. Księga I. Część ogólna, J. Gutowski (red.), Warszawa 2016, komentarz do art. 23 k.c., teza 13).

Przedstawione rozumienie dobra osobistego tj. prywatności rodzi ryzyko wąskiego ujęcia w jej ramach danych osobowych (m.in. pojawia się wątpliwość czy w ramach art. 24 § 1 k.c. można żądać, ażeby osoba, która dopuściła się naruszenia np. odmówiła wydania kopii danych, dopełniła czynności potrzebnych do usunięcia jego skutków). W związku z tym projektodawca zdecydował się na wprowadzenie regulacji odrębnej w art. 78 ust. 1 projektu, dającej wyraźną cywilnoprawną podstawę roszczeń o charakterze niemajątkowym. Dochodzenie roszczeń powiązano z naruszeniem praw podmiotów danych wynikających z przepisów o ochronie danych osobowych (nie tylko Rozporządzenia). W ten sposób, bez potrzeby definiowania dobra osobistego (danych osobowych) skonstruowano podstawę dochodzenia cywilnoprawnych roszczeń niemajątkowych w razie naruszenia praw przysługujących na podstawie przepisów o ochronie danych osobowych.

Należy zwrócić w tym miejscu uwagę, iż art. 78 ust. 1 projektu dotyczy wyłącznie dokonanego naruszenia praw przysługujących na mocy przepisów o ochronie danych osobowych. W tej sytuacji przysługiwać będzie roszczenie o:

- zaniechanie tego działania;

- to aby ten kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków.

Projektowany art. 79 ust. 1 ma charakter porządkowy i przesądza cywilnoprawny tryb dochodzenia roszczeń wskazanych w art. 78 projektu. Natomiast celem art. 79 ust. 2 jest przyznanie sądom okręgowym właściwości w sprawach roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w tym roszczeń z tytułu art. 82 Rozporządzenia. 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. Przepis ten stanowi regulację szczególną względem art. 17 pkt 4 kodeksu postępowania cywilnego.

Celem wprowadzenia art. 80 oraz 81 projektu jest udrożnienie i przyspieszenie komunikacji pomiędzy sądami powszechnymi a Prezesem Urzędu. Należy zwrócić uwagę, iż wniesienie pozwu w sprawach, o których mowa w art. 78 projektu obliguje sąd – przed którym toczy się postępowanie - do zawiadomienia Prezesa Urzędu. Niemniej sąd może ale nie musi zawiesić toczącego się przed nim postępowania.

Przepisy **Rozdziału 9** projektu dotyczą administracyjnych kar pieniężnych. 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.

Na gruncie projektu ustawy przyjęto, iż w polskim systemie prawnym przez organy publiczne będą rozumiane organy administracji publicznej w rozumieniu art. 5 § 2 pkt 3 Kodeksu, a więc: ministrowie, centralne organy administracji rządowej, wojewodowie, działające w ich lub we własnym imieniu inne terenowe organy administracji rządowej (zespolonej i niezespolonej), organy jednostek samorządu terytorialnego oraz organy i podmioty wymienione w art. 1 pkt 2 Kodeksu. Przez podmioty publiczne będziemy natomiast rozumieli podmioty sektora finansów publicznych a więc:

1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;

2) jednostki samorządu terytorialnego oraz ich związki;

2a) związki metropolitalne;

3) jednostki budżetowe;

4) samorządowe zakłady budżetowe;

5) agencje wykonawcze;

6) instytucje gospodarki budżetowej;

7) państwowe fundusze celowe;

8) Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;

9) Narodowy Fundusz Zdrowia;

10) samodzielne publiczne zakłady opieki zdrowotnej;

11) uczelnie publiczne;

12) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;

13) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

Polski prawodawca skorzystał z możliwości jaką daje art. 83 ust. 7 Rozporządzenia i w przepisie art. 83 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 i wysokość kar nie może przekroczyć 100 000 zł.

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 spełniałyby 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, wyłączając z możliwości objęcia takimi karami państwowe i samorządowe instytucje kultury. 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. Państwowe i samorządowe instytucje kultury, a także jednostki zakładane i prowadzone przez osoby fizyczne czy fundacje i stowarzyszenia, dysponują z reguły niewielkimi budżetami, a jednocześnie zakres przetwarzanych danych osobowych nie powoduje znaczącego zagrożenia dla prywatności użytkowników. 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 Prawa zamówień publicznych (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 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 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 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 (vide art. 21 ust.1 pkt 68 i 132, art. 22 ust. 9 pkt 3 i art. 26 ust.1 lit. a ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych czy art. 18 ust.1 pkt 1 ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych). 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 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 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.

Nową instytucją w polskim systemie prawnym jest Fundusz Ochrony Danych Osobowych będący państwowym funduszem celowym. Przychodami Funduszu ma być 1% administracyjnych kar pieniężnych a wydatki Funduszu mają być przeznaczane na cele wskazane w art. 87 ust. 4 projektu. Celem powołania tej instytucji jest zapewnienie finansowania przedsięwzięć oraz udostępnianie wiedzy z zakresu ochrony danych osobowych.

Rozdział 10 projektu wprowadza do projektu przepisy karne. Generalnie celem projektodawcy było nie rozbudowywanie 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 w trybie przepisów Kodeksu postępowania w sprawach o wykroczenia. Sankcją jest kara grzywny. Uznano te działania za czyn mniejszej wagi niż działania opisane w art. 91 projektu. Przepis ten penalizuje przetwarzanie pewnych szczególnych kategorii danych (z art. 9 Rozporządzenia) bez podstawy prawnej. Mając na względzie dobro podmiotów danych oraz wagę naruszenia, jakim jest przetwarzanie danych dotyczących, np. zdrowia, czy seksualności, uznano, że przetwarzanie ich bez podstawy prawnej, a więc nieuprawnione przetwarzanie, powinno być zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku. Tak więc orzekanie w tych sprawach będzie odbywało się w trybie przepisów Kodeksu postępowania karnego.

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".

W art. 91 projektu ustawy zawarto regułę wydatkową zgodnie z art. 50 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Wskazane kwoty zostały oparte na zawartych w dołączonej do projektu ocenie skutków regulacji i wskazują one różnice w wydatkach budżetu państwa w stosunku do kwot zaplanowanych w ustawie budżetowej.

Ustawa wejdzie w życie w terminie wskazanym w ustawie – Przepisy wprowadzające ustawę o finansach publicznych.

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.

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 Ministra Cyfryzacji.

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** Anna Streżyńska Minister Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Dr Maciej Kawecki, Zastępca Dyrektora Departamentu Zarządzania Danymi w Ministerstwie Cyfryzacji maciej_kawecki@mc.gov.pl	**Data sporządzenia** 18.08.2017 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, poprzez 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 przyjęcia 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 takich, 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 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 informuje o trudnościach w udzielaniu porad prawnych. Brak jest również infolinii, która dotychczas funkcjonowała i obsługiwała liczne wątpliwości adresowane przez obywateli.

Do dnia opracowania przedmiotowego dokumentu (21 lipca 2017 r.), Generalny Inspektor Ochrony Danych Osobowych nie złożył w Sejmie sprawozdania ze swojej działalności w roku 2016 w związku z powyższym, wykorzystywane w dokumencie dane pochodzą ze sprawozdania z 2015 r.

Zakres przedmiotowy projektu nowej ustawy o ochronie danych nie obejmie również tych wszystkich zagadnień, które są objęte regulacją rozporządzenia 2016/679, a które na gruncie przepisów krajowych są uregulowane w ustawach szczególnych.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

1. W projekcie ustawy o ochronie danych osobowych określono zakres podmiotowy, przedmiotowy i terytorialny projektowanej ustawy. Ustawa będzie miała zastosowanie do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Wobec powyższego przepisy ustawy nie znajdą zastosowania do ochrony innych podmiotów w związku z przetwarzaniem ich danych osobowych. W projekcie ustawy przyjęto, że przedmiotowy zakres jej zastosowania będzie odpowiadał zakresowi zastosowania rozporządzenia 2016/679. Stosowanie ustawy 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.
2. Projektodawca skorzystał z przewidzianej w art. 8 rozporządzenia 2016/679 możliwości obniżenia wieku dziecka z lat 16 do lat 13, gdy na przetwarzanie jego danych osobowych w usługach społeczeństwa informacyjnego konieczne będzie uzyskanie zgody rodzica bądź opiekuna prawnego. Zgodnie z art. 15 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. z 2016 r. poz. 380, z późn. zm.) osoba, która ukończyła 13 lat ma ograniczoną zdolność do czynności prawnych, a zatem może zawierać umowy w drobnych bieżących sprawach życia codziennego, może także rozporządzać swoim zarobkiem. W ocenie projektodawcy w tym kontekście uzasadnione jest przyjęcie granicy lat 13 także dla skutecznego wyrażenia przez dziecko zgody na przetwarzanie dotyczących go danych osobowych, w związku z kierowanymi bezpośrednio do dziecka usługami społeczeństwa informacyjnego. Nie ma powodu, aby przyjąć, że osoba mogąca rozporządzić swoim zarobkiem oraz zawierać drobne umowy, nie była jednocześnie uprawniona do wyrażenia zgody na przetwarzanie dotyczących jej danych osobowych, szczególnie, że zgodnie z przepisami rozporządzenia 2016/679 zgodę można w każdym czasie wycofać.
3. Uregulowano tryb notyfikacji inspektorów ochrony danych osobowych oraz podmioty obowiązane w polskim porządku prawnym do wyznaczenia inspektora ochrony danych osobowych.
4. Uregulowano zasady certyfikacji oraz tryb postępowania w tych sprawach. W projekcie ustawy zaproponowano by w polskim systemie prawnym certyfikacji udzielał organ nadzorczy, a więc Prezes Urzędu Ochrony Danych Osobowych wg kryteriów określonych przez Prezesa Urzędu, z uwzględnieniem art. 43 ust. 2 rozporządzenia 2016/679, i opublikowanych w Biuletynie Informacji Publicznej.
5. Rozporządzenie 2016/679 wymusza na państwach członkowskich stworzenie nowego krajowego systemu ochrony danych osobowych, na czele z organem nadzorczym, którym według projektodawcy powinien być Prezes Urzędu Ochrony Danych Osobowych. Zgodnie bowiem z motywem 117 rozporządzenia 2016/679 *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*. W związku z powyższym, z chwilą wejścia w życie nowej ustawy o ochronie danych osobowych utworzony zostanie taki nowy organ nadzorczy, który w zakresie swoich kompetencji, w tym do nakładania administracyjnych kar finansowych, będzie znacznie różnił się od Generalnego Inspektora. Projekt ustawy ustanawia więc jak zostało to wskazane, nowy organ nadzorczy – Prezesa Urzędu Ochrony Danych Osobowych. Nowy organ ochrony danych osobowych będzie nie tylko organem nadzorczym w rozumieniu rozporządzenia 2016/679 lecz ze znacznie szerszym zakresem uprawnień i obowiązków niż dzisiejszy GIODO, ale będzie również organem nadzorczym 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 uchylająca decyzję ramową Rady 2008/977/WSiSW.
6. W projekcie ustawy uregulowano tryb postępowania w sprawach naruszenia przepisów o ochronie danych osobowych. Jak zostało to już wskazane, obecny czas trwania postępowania w sprawie naruszenia przepisów o ochronie danych osobowych jest zbyt długi. Założeniem przyświecającym Ministrowi Cyfryzacji jest, więc przyśpieszenie trwających postępowań poprzez utrzymanie terminów wynikających z ustawy z dnia 14 czerwca 1960 r. Kodeks

postępowania administracyjnego, zasadą jest więc wydanie rozstrzygnięcia niezwłocznie. Celem przyśpieszenia postępowania jest projekt, który znosi dwuinstancyjności postępowania w sprawach naruszenia przepisów o ochronie danych osobowych. Zniesienie dwuinstancyjności ma zapewnić obywatelom możliwość szybszego uzyskania sądowej ochrony swoich praw. Organowi przyznane zostanie jednak uprawnienie do autokontroli wydanej decyzji. Kolejnym celem przyśpieszenia postępowań prowadzonych w związku z naruszeniami przepisów o ochronie danych osobowych jest wprowadzenie do ustawy przepisu, w świetle którego postępowanie kontrolne w sprawach naruszenia ochrony danych nie może trwać dłużej niż miesiąc.

7. Założeniem jest stworzenie organu będącego nie tylko podmiotem sprawnie egzekwującym wszelkie naruszenia zasad ochrony danych, ale również otwartym i służącym udzielaniu porad nie tylko obywatelom, ale również przedsiębiorcom – jak postępować by skuteczniej chronić naszą prywatność. Projekt nakłada, więc na Prezesa Urzędu obowiązek wydawania rekomendacji adresowanych do przedsiębiorców w zakresie zasad zabezpieczania danych osobowych. Przedmiotem projektu ustawy o ochronie danych osobowych są też 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 świadczonych drogą elektroniczną, certyfikacji oraz sądowej ochrony praw przysługujących. Przepisy ustawy wprowadzającej ustawę o ochronie danych osobowych zawierają z kolei szereg zmian sektorowych wypracowanych wspólnie z właściwymi resortami, zapewniającymi obszary takie jak sektor bankowy, ubezpieczeniowy, wymiar sprawiedliwości, sektor kultury, statystyka publiczna czy zasady przetwarzania danych osobowych pracowników przez pracodawców.

8. Projekt ustawy reguluje również kwestie odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych. Art. 79 ust. 1 rozporządzenia 2016/679 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 2016/679 zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem rozporządzenia.

9. Rozporządzenie 2016/679 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 2016/679. Jednocześnie brak jest jednak jakiegokolwiek związku ustrojowego pomiędzy takimi osobami a przyszłym organem nadzorczym, odpowiadającym za egzekwowanie w Polsce przestrzegania przepisów rozporządzenia 2016/679. Przyjęcie obecnej nazwy organu wprowadzałoby w tym zakresie w błąd, w tym co do ich pozycji ustrojowej. Zgodnie z art. 38 ust. 3 rozporządzenia 2016/679 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 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 niedopuszczalne. Uwzględniając powyższe, odstąpiono również od nazywania w projekcie pracowników organu nadzorczego przeprowadzających w jego imieniu czynności kontrolne inspektorami, na rzecz nazwania ich kontrolującymi. Rozwiązanie takie na etapie prowadzonych prekonsultacji uzyskało aprobatę znacznej liczby podmiotów w tym stowarzyszeń zrzeszających administratorów bezpieczeństwa informacji oraz izb gospodarczych (np. Izba Gospodarki Elektronicznej).

10. W projekcie ustawy uregulowano również kwestie dotyczące administracyjnych kar pieniężnych. Należy wskazać, iż przesłanki nakładania kar jak również ich maksymalne wysokości wynikają wprost z rozporządzenia 2016/679 (art. 83 ust. 1 – 6). Prawodawca unijny wprowadził jednak możliwość szczególnego uregulowania przez państwa członkowskie kwestii nakładania kar na organy i podmioty publiczne. Każde państwo członkowskie może bowiem 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 2016/679 i w przepisie art. 75 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 i wysokość kar nie może przekroczyć 100 000 zł.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Rozporządzenie 2016/679 jest co do zasady, aktem prawnym bezpośrednio obowiązującym, tak więc będzie miało bezpośrednie zastosowanie we wszystkim państwach członkowskich Unii Europejskiej. Najważniejszym celem reformy europejskich przepisów o ochronie danych osobowych jest bowiem zapewnienie w całej Unii spójnego i jednolitego poziomu ochrony danych osób fizycznych, tak aby umożliwić swobodny przepływ danych osobowych w Unii oraz ułatwić funkcjonowanie przedsiębiorstw na jednolitym rynku.

W konsekwencji wszystkie państwa członkowskie UE będą stosowały przepisy ww. rozporządzenia. Jednocześnie jednak niniejsze rozporządzenie, szanując odmienności porządków i tradycji prawnych poszczególnych państw członkowskich UE, pozostawia pewne kwestie do uregulowania i doprecyzowania w prawie krajowym poszczególnych państw członkowskich.

W efekcie w pozostałych państwach członkowskich UE, analogicznie jak w przypadku Polski, prowadzone są niezbędne prace wdrożeniowe, polegające na przeglądzie i dostosowaniu (zmianie bądź uchyleniu) przepisów krajowych z zakresu ochrony danych osobowych do nowych wymogów, jakie nakłada niniejsze rozporządzenie.
W przypadku ogromnej większości państw prace jeszcze trwają, a projekty aktów prawnych wdrażających rozporządzenie 2016/679 są na etapie prac rządowych bądź konsultacji publicznych. Stąd też obecnie, poza dwoma wyjątkami, brak jest rozwiązań z innych państw członkowskich, które mogłyby być przedmiotem analizy. Większość państw planuje skierowanie projektu do prac parlamentarnych jesienią 2017 r.
Państwami, w których już uchwalono przepisy wdrażające rozporządzenie 2016/679 są Niemcy[1] i Austria[2].
Niemiecki akt prawny wdrażający rozporządzenie 2016/679 stanowi wdrożenie zarówno rozporządzenie ogólnego jak i tzw. dyrektywy policyjnej[3], czyli obu elementów pakietu reformującego unijne zasady ochrony danych osobowych. Niemiecka ustawa nie zawiera jednak zmian w przepisach sektorowych, które będą procedowane przez rząd niemiecki na późniejszym etapie. Niemiecka ustawa zawiera m.in. szczegółowe przepisy dotyczące przetwarzania danych pracowników, czy przetwarzania danych wrażliwych. Niemiecka ustawa dodatkowo obliguje każde przedsiębiorstwo zatrudniające co najmniej 10 pracowników do wyznaczenia inspektora ochrony danych, a w zakresie sankcji dodatkowo sankcjonuje (do 50 000 EUR) naruszenia przepisów o ochronie danych w obszarze kredytów konsumenckich. Wychodzi ona także poza zakres ogólnego rozporządzenia, regulując m.in. kwestię monitoringu wizyjnego, czy też – zgodnie z wyrokiem Trybunału Sprawiedliwości w sprawie C-362/14, dopuszczając możliwość zakwestionowania przez organ nadzorczy tzw. decyzji o adekwatności wydawanych przez Komisję Europejską.
Wśród rozwiązań zawartych w austriackiej ustawie warto odnotować m.in. objęcie ochroną z tytułu ochrony danych osobowych również osób prawnych czy ustanowienie zgody dziecka na przetwarzanie danych w celu korzystania z usług społeczeństwa informacyjnego na 14 lat.
Odnośnie do państw OECD, warto zaznaczyć, że wdrożenie rozporządzenia 2016/679, jako aktu unijnego, nie dotyczy państw OECD nie będących członkami Unii Europejskiej. Państwami spoza UE, które będą stosować rozporządzenie 2016/679 są również Islandia, Lichtenstein i Norwegia, co ma miejsce w związku z ich przynależnością do Europejskiego Obszaru Gospodarczego. Również i Wielka Brytania, pomimo Brexitu, zdecydowała się w pełni wdrożyć przepisy rozporządzenia 2016/679.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty prowadzące działalność polegającą na publikowaniu materiałów prasowych.	Ok. 3000	Dane z krajowego rejestru urzędowego podmiotów gospodarki narodowej REGON na dzień 30 czerwca 2017 r.	Zmniejszenie obowiązków ciążących na podmiotach prowadzących działalność polegającą na publikowaniu materiałów prasowych, względem wynikających z rozporządzenia 2016/679. Niezależnie od powyższego, rozporządzenie 2016/679 przewiduje szereg obowiązków nakładanych na takie podmioty przyznając również organowi nadzorczemu uprawnienie do nakładania administracyjnych kar finansowych.
Podmioty prowadzące działalność literacką oraz artystyczną.	Ok. 20000	Informacje o liczbie przedsiębiorców, według stanu rejestru REGON na dzień 30.06.2017 r.	Zmniejszenie obowiązków ciążących na podmiotach prowadzących działalność literacką oraz artystyczną, względem wynikających z rozporządzenia 2016/679.

[1]Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680.
[2] Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DatenschutzAnpassungsgesetz 2018)
[3] Dyrektywa 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

Przedsiębiorcy	Ok. 3440000	Informacje o liczbie przedsiębiorców, według stanu rejestru REGON na dzień 30.06.2017 r.	Obowiązek notyfikacji inspektorów ochrony danych do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku przedsiębiorców których główna działalność polega na regularnym i systematycznym monitorowaniu osób, których dane dotyczą, na dużą skalę lub główna działalność polega na przetwarzaniu danych szczególnie chronionych na dużą skalę oraz danych dotyczących skazań.
Stowarzyszenia, inne organizacje społeczne i zawodowe, fundacje oraz samodzielne publiczne zakłady opieki zdrowotnej.	Ok. 110000	Informacje o liczbie przedsiębiorców, według stanu rejestru REGON na dzień 30.06.2017 r.	Obowiązek notyfikacji inspektorów ochrony danych do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku przedsiębiorców których główna działalność polega na regularnym i systematycznym monitorowaniu osób, których dane dotyczą, na dużą skalę lub główna działalność polega na przetwarzaniu danych szczególnie chronionych na dużą skalę oraz danych dotyczących skazań.
Administracja publiczna	Ok. 68000	Informacje o liczbie podmiotów, według stanu rejestru REGON na dzień 30.06.2017 r. oraz dane z powszechnie dostępnej bazy administratorów bezpieczeństwa informacji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych. Spośród 68 000 podmiotów publicznych, w przybliżeniu około 18 000 z nich powołało już dzisiaj administratora bezpieczeństwa informacji. Pozostaje w przybliżeniu około 50 000 podmiotów, które będą zobowiązane do wyznaczenia inspektora ochrony danych nie mając w swoich zasobach administratora bezpieczeństwa informacji.	- Obowiązek notyfikacji inspektorów ochrony danych do Prezesa Urzędu Ochrony Danych Osobowych. - Przepisy wymuszają prowadzenie współpracy pomiędzy organami administracji publicznej w zakresie odniesienia się do wystąpień kierowanych przez Prezesa Urzędu oraz odpowiedzi na wnioski o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych.
Prezes Urzędu Ochrony Danych Osobowych	1		- Ustawa nakłada na Prezesa Urzędu szereg obowiązków, których spełnienie wymusza zwiększenie liczby zatrudnionych pracowników (co najmniej dwukrotne względem dzisiejszej liczby) z uwagi na dużą liczbę nowych, nie istniejących w obowiązującym

			stanie prawnym obowiązków. Wprowadzony zostaje obowiązek notyfikacji inspektorów ochrony danych, a liczba podmiotów zobowiązanych do takiej notyfikacji sięgać będzie dziesiątek tysięcy. Przepisy nakładają również obowiązek certyfikacji przez Prezesa Urzędu. Prezes Urzędu udostępniał będzie również w Biuletynie Informacji Publicznej kryteria certyfikacji. Prezes Urzędu będzie również brał udział w procedurze legislacyjnej wymagającej dokonywania bieżącej analizy projektowanych aktów prawnych w Polsce dotyczących ochrony danych osobowych i ich opiniowania. Prezes Urzędu podejmował będzie również działania w zakresie zatwierdzania kodeksów postępowań oraz dobrych praktyk. Prezes Urzędu dokonywał będzie również akredytacji podmiotów monitorujących kodeksy postępowań. Prezes Urzędu wydawał będzie również komunikat zawierający wykaz operacji przetwarzania danych osobowych podlegających wymogowi oceny skutków. Organ będzie gromadził oraz ewidencjonował notyfikacje naruszeń ochrony danych osobowych. Zwiększa się liczba uprawnień osób, których dane dotyczą, a tym samym zwiększy się liczba skarg składanych do Prezesa Urzędu. Prezes Urzędu będzie również organem zobowiązanym do prowadzenia współpracy administracyjnej z innymi organami ochrony danych osobowych państw członkowskich. Konieczne jest również skrócenie czasu trwania postępowań w sprawie naruszeń przepisów o ochronie danych osobowych względem obecnego stanu faktycznego. Powyższe wymusza zwiększenie liczby osób zatrudnionych w biurze Prezesa Urzędu Ochrony Danych

			Osobowych co najmniej poprzez ich podwojenie. -Wymóg elektronizacji systemów, utrzymania i modyfikacji systemu teleinformatycznego notyfikacji naruszeń, systemu notyfikacji danych kontaktowych inspektorów ochrony danych, systemu zarządzania dokumentacją oraz systemu rozliczeń z ukaranymi. - Działania podjęte w związku z następstwem prawnym, gdzie Generalnego Inspektora Ochrony Danych Osobowych zastąpi Prezes Urzędu Ochrony Danych Osobowych. Wymiana tablicy emaliowanej z nazwą urzędu, zmiana nazwy na wewnętrznych tablicach informacyjnych, zmiana metalowych pieczęci urzędowych, zmiana wizytówek oraz pieczątek pracowników. - Powołanie przy Prezesie Urzędu Ochrony Danych Osobowych Rady do Spraw Ochrony Danych Osobowych.
Sądy Powszechne	317 sądów rejonowych, 45 sądy okręgowe, 11 sądów apelacyjnych.		- Przepisy przyznają nową podstawę prawną do kierowania pozwów z tytułu naruszenia przepisów o ochronie danych osobowych do sądów okręgowych. Uwzględniając instancyjną strukturę polskiego wymiaru sprawiedliwości oraz ustanowienie nowej podstawy prawnej kierowania pozwów w sprawach o roszczenia wynikające z naruszenia przepisów o ochronie danych osobowych do sadów powszechnych, należy spodziewać się zwiększenia liczby spraw kierowanych do sądów powszechnych różnych szczebli oraz Sądu Najwyższego.
Obywatele	Ok. 38424000	Dane statystyczne Głównego Urzędu Statystycznego.	- Przepisy przyznają obywatelom nowe uprawnienia w szczególności w zakresie kierowania do sądu powszechnego pozwu z tytułu naruszenia przepisów o ochronie danych osobowych, złożenia skargi do Prezesa Urzędu. Postępowanie w

			sprawie naruszenia przepisów o ochronie danych ma być również prowadzone szybciej. - Uregulowanie materii prawnej związanej z odpowiedzialnością, administracją i nadzorem nad systemami teleinformatycznymi oraz postępowaniami prowadzonymi w formie papierowej w wymiarze sprawiedliwości zapewniającymi bezpieczne przetwarzanie danych osobowych.
Sąd Najwyższy	1		- Przepisy przyznają nową podstawę prawną do kierowania pozwów z tytułu naruszenia przepisów o ochronie danych osobowych do sądów okręgowych. Uwzględniając instancyjną strukturę polskiego wymiaru sprawiedliwości oraz ustanowienie nowej podstawy prawnej kierowania pozwów w sprawach o roszczenia wynikające z naruszenia przepisów o ochronie danych osobowych do sadów powszechnych, należy spodziewać się zwiększenia liczby spraw, kierowanych do sądów powszechnych różnych szczebli oraz Sądu Najwyższego.
Sądy administracyjne	16 Wojewódzkich Sądów Administracyjnych i Naczelny Sąd Administracyjny		- Rozpatrywanie skarg od decyzji Prezesa Urzędu;

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Od samego początku podejmowanych w Ministerstwie Cyfryzacji działań zmierzających do zapewnienia skutecznego stosowania rozporządzenia 2016/679, celem było zapewnienie im pełnej transparentności. Projektowane rozwiązania krajowe dotyczą bowiem ochrony prawa podstawowego i mają ogromny wpływ na niemal każdy obszar działania państwa. Jej wyrazem było chociażby organizowanie w Ministerstwie Cyfryzacji szeregu otwartych spotkań transmitowanych on–line na stronie internetowej Ministerstwa Cyfryzacji. Na spotkaniach każda ze zgromadzonych osób mogła zadać każde pytanie, dotyczące podejmowanych w Ministerstwie Cyfryzacji działań legislacyjnych. W dniu 3 lutego 2017 r. odbyło się takie spotkanie dedykowane wprost dla przedsiębiorców, a w dniu 29 maja 2017 r. spotkanie z przedstawicielami organizacji pozarządowych zainteresowanych tematyką unijnej oraz krajowej reformy ochrony danych osobowych. W spotkaniu aktywnie uczestniczyły organizacje takie jak chociażby Helsińska Fundacja Praw Człowieka, Amnesty International, Fundacja im. Stefana Batorego, Pracodawcy RP, Sieć Obywatelska Watchdog Polska, Przewodnicząca Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej, Fundacja ePaństwo oraz Centrum Cyfrowe. W dniu 2 lutego 2017 r. w Ministerstwie Cyfryzacji odbyło się spotkanie kierownictwa Ministerstwa Cyfryzacji z przedstawicielami kościołów oraz związków wyznaniowych, by rozmawiać na temat nowych zasad przetwarzania przez nie danych osobowych. W spotkaniu mógł wziąć udział każdy zarejestrowany na terytorium Polski kościół oraz związek wyznaniowy. W dniu 9 grudnia 2016 r. w Ministerstwie Cyfryzacji zorganizowano spotkanie pracowników resortu z przedstawicielami środowiska naukowego zajmującymi się ochroną danych osobowych. W trakcie spotkania naukowcy przedstawili swoje doświadczenia w zakresie zagadnień związanych ze stosowaniem obowiązujących obecnie przepisów o ochronie danych

osobowych oraz poglądy dotyczące nowych unijnych ram prawnych ochrony danych osobowych. Pracownicy Ministerstwa Cyfryzacji niemal każdego dnia uczestniczą w Ministerstwie Cyfryzacji w spotkaniach z organizacjami, obywatelami oraz izbami gospodarczymi zainteresowanymi unijną reformą ochrony danych osobowych. Od początku podejmowanych działań legislacyjnych, pracownicy Ministerstwa Cyfryzacji uczestniczyli również w kilkudziesięciu konferencjach naukowych, forach, warsztatach poświęconych reformie ochrony danych osobowych. Celem takich działań jest czynne uczestnictwo Ministerstwa Cyfryzacji w debacie publicznej, poświęconej reformie ochrony danych osobowych. W dniu 28 marca br. na stronie internetowej Ministra Cyfryzacji udostępniony został również projekt części przepisów projektowanej ustawy o ochronie danych osobowych. Decyzja o udostępnieniu wypracowanych w dacie ich udostępnienia części przepisów projektu podyktowana została dużym zainteresowaniem społecznym wypracowywanymi zmianami prawnymi i chęcią zapewnienia procesowi tworzenia nowych przepisów pełnej transparentności. Efektem powyższych działań, było zebranie przez Ministerstwo Cyfryzacji ogromnej ilości postulatów, założeń co do polskiego systemu ochrony danych osobowych, które podlegały wnikliwej ocenie i miały wpływ na kształt projektu przepisów o ochronie danych.

Projekty ustaw zostaną udostępnione w Biuletynie Informacji Publicznej na stronie internetowej Rządowego Centrum legislacji w zakładce Rządowy Proces Legislacyjny i poddane uzgodnieniom z wszystkimi członkami Rady Ministrów. Projekty ustaw będą również przedmiotem opiniowania i konsultacji przeprowadzanych jednocześnie z uzgodnieniami międzyresortowymi. Czas trwania konsultacji przewidziany został na 30 dni. Projekty ustaw z zaproszeniem do możliwości zgłaszania uwag zamieszczone zostaną również na stronie internetowej Ministerstwa Cyfryzacji oraz na platformie internetowej służącej konsultacjom publicznym www.konsultacje.gov.pl. W ramach opiniowania projekty ustaw zostaną przekazane Komisji Wspólnej Rządu i Samorządu Terytorialnego, Komitetowi Rady Ministrów do Spraw Cyfryzacji, Komitetowi Ekonomicznemu Rady Ministrów.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	**0**
JST	0	0	0	0	0	0	0	0	0	0	0	**0**
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	**0**
Wydatki ogółem	**27,214**	**16,298**	**16,509**	**16,285**	**16,515**	**16,285**	**16,516**	**16,285**	**16,515**	**16,285**	**18,015**	**192,722**
budżet państwa	26,800	16,113	16,093	16,100	16,100	16,100	16,100	16,100	16,100	16,100	17,600	**189,306**
JST	0,000	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	**0,010**
pozostałe jednostki (oddzielnie)	0,414	0,184	0,415	0,184	0,414	0,184	0,415	0,184	0,414	0,184	0,414	**3,406**
Saldo ogółem	**-27,214**	**-16,298**	**-16,509**	**-16,285**	**-16,515**	**-16,285**	**-16,516**	**-16,285**	**-16,515**	**-16,285**	**-18,015**	**-192,722**
budżet państwa	-26,800	-16,113	-16,093	-16,100	-16,100	-16,100	-16,100	-16,100	-16,100	-16,100	-17,600	**-189,306**
JST	0,000	-0,001	-0,001	-0,001	-0,001	-0,001	-0,001	-0,001	-0,001	-0,001	-0,001	**-0,010**
pozostałe jednostki (oddzielnie)	-0,414	-0,184	-0,415	-0,184	-0,414	-0,184	-0,415	-0,184	-0,414	-0,184	-0,414	**-3,406**

Źródła finansowania	Przewidziane w niniejszym dokumencie skutki finansowe powinny pochodzić odpowiednio z budżetu państwa i JST. Przepisy rozporządzenia 2016/679 nie wpłyną bezpośrednio na realizację zadań przez jednostki samorządu terytorialnego i nie generują nowych zadań publicznych w związku z czym nie powoduje to konieczności zmiany w podziale dochodów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wskazany w Ocenie Skutków Regulacji wpływ na sektor finansów publicznych obejmuje wyłącznie koszty związane z nadwyżką środków koniecznych do wydatkowania w związku z projektowaną regulacją. W związku z powyższym, wskazane kwoty związane z funkcjonowaniem Prezesa Urzędu Ochrony Danych Osobowych powinny zostać powiększone odpowiednio o kwotę w 21 mln zł (źródło: plan finansowy Generalnego Inspektora Ochrony Danych Osobowych na rok 2017, www.giodo.gov.pl) **Projekt ustawy o ochronie danych osobowych**

2.1. Skutki przewidziane w tabeli w okresie 10 lat od wejścia w życie zmian

1.1.1. Koszty związane z funkcjonowaniem Prezesa Urzędu Ochrony Danych Osobowych

- Koszty związane z następstwem prawnym, gdzie Generalnego Inspektora Ochrony Danych Osobowych zastąpi Prezes Urzędu Ochrony Danych Osobowych. Koszt wymiany tablicy emaliowanej z nazwą urzędu w przybliżeniu 770 zł, koszt zmiany nazwy wewnętrznej tablicy informacyjnej w przybliżeniu 540 zł, wymiana 5 szt. metalowych pieczęci urzędowych w przybliżeniu 2 500 zł, wykonanie nowych obwolut na dokumenty w przybliżeniu 2 500 zł, zakup materiałów promocyjnych 3 500 zł, koszt nowej pieczątki + wizytówek dla wszystkich pracowników – ok 160 zł/os. Łączny koszt poniesionych wydatków to w przybliżeniu to 33 000 zł, przy uwzględnieniu wskazanej poniżej konieczności zatrudnienia w Urzędzie Ochrony Danych Osobowych dodatkowych 145 osób.
- Ustawa nakłada na Prezesa Urzędu szereg obowiązków, których spełnienie wymusza zwiększenie liczby zatrudnionych pracowników (co najmniej dwukrotne względem dzisiejszej liczby) z uwagi na dużą liczbę nowych, nie istniejących w obowiązującym stanie prawnym obowiązków. W chwili obecnej w oparciu na sprawozdanie Generalnego Inspektora z 2015 r. liczba pracowników wyniosła 145, 5 etatu. Bez wątpienia wzrośnie ilość spraw rozpatrywanych przez Prezesa Urzędu. Po pierwsze, samo rozporządzenie 2016/679 przyznaje obywatelom ponad 20 nowych uprawnień, w tym prawo do sprzeciwu przed podejmowaniem automatycznych decyzji opartych na profilowaniu, prawo do bycia zapomnianym czy prawo do żądania przeniesienia danych osobowych. Wiązało się to będzie zwiększenie ilości skarg w związku z nienależytym wykonywaniem nowo przyznanych uprawnień. Przepisy nakładają również na wszystkich przedsiębiorców oraz wszystkie podmioty publiczne obowiązek w przypadku naruszenia ochrony danych osobowych, zgłaszania faktu naruszenia organowi nadzorczemu w ciągu 72 h. W obowiązującym stanie prawnym obowiązek taki ciąży wyłącznie na operatorach telekomunikacyjnych. Ze sprawozdania Generalnego Inspektora z 2015 r. wynika, że otrzymał on 93 takie notyfikacje w 2015 r. Liczba przedsiębiorców telekomunikacyjnych na dzień 11 lipca 2017 r. znajdujących się w Rejestrze Przedsiębiorców Telekomunikacyjnych wynosi 6 023 podmiotów. Opierając się na danych z rejestru REGON, że liczba przedsiębiorstw, organów administracji publicznej oraz stowarzyszeń i fundacji wynosi łącznie w przybliżeniu 3 600 000, liczba podmiotów zobowiązanych do takich notyfikacji wzrasta 600 krotnie. Liczba notyfikacji naruszeń w ciągu roku sięgnąć może, więc 55 000, czyli w przybliżeniu 4 600 notyfikacji miesięcznie. Z czego każda powinna podlegać odrębnej ocenie z punktu widzenia zasadności wszczęcia przez Prezesa Urzędu postępowania z urzędu. Decyzja o wszczęciu generowała będzie z kolei potrzebę obsługi takich postępowań. Liczba notyfikacji inspektorów ochrony danych kierowanych do Prezesa Urzędu Ochrony Danych może wynieść w przybliżeniu tylko od administracji publicznej ok. 50 000 notyfikacji. Przepisy rozporządzenia 2016/679 przewidują mechanizmy certyfikacji, a projekt ustawy o ochronie danych osobowych je uzupełnia. Projekt nakłada na Prezesa Urzędu Ochrony Danych Osobowych obowiązek certyfikacji. Podejmowanie takich działań wiąże się z kosztami po stronie organu związanymi z koniecznością zatrudnienia odpowiedniej liczby osób podejmujących czynności certyfikacji. Uwzględniając wskazaną już konieczność, co najmniej podwojenia ilości zatrudnionych pracowników, podwojeniu powinna ulec kwota obecnie wydatkowana na takie cele przez Generalnego Inspektora Ochrony Danych Osobowych. Na podstawie informacji wynikających z sprawozdania organu z 2015 r. budżet Generalnego Inspektora na wynagrodzenia wyniósł 10 156 000 zł, a na pochodne od wynagrodzeń 1 798 000 zł. Łącznie stanowi to kwotę 11 954 000 zł. Wskazane powyżej powiększenie liczby etatów nie obejmuje koniecznych do zatrudnienia pracowników IT w związku ze zmianami w systemach informatycznych Prezesa Urzędu, które zostały wykazane w dalszej części OSR, poświęconej zmianie systemów IT. Powyższy wykaz nie obejmuje zadań nałożonych na Prezesa Urzędu projektowaną przez Ministra Spraw Wewnętrznych i Administracji ustawą implementującą 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. Skutki kadrowe powyższych działań przewidziane zostaną w Ocenie Skutków Regulacji dołączonej do projektu ustawy tworzonego przez Ministra Spraw Wewnętrznych i Administracji.
- Koszty związane z utrzymaniem przez Prezesa Urzędu Ochrony Danych Osobowych Rady do Spraw Ochrony Danych Osobowych. Opierając się na wydatkach podejmowanych przez Ministra Cyfryzacji w związku z funkcjonowaniem Rady do Spraw Cyfryzacji, koszt wynagrodzenia

	przewodniczącego za udział w posiedzeniu wynosi 400 zł, członka 350 zł. Przyjmując, że Rada do Spraw Ochrony Danych Osobowych spotykałaby się raz w miesiąc, łączny roczny koszt wynagrodzeń jej 8 członków wyniósłby 34 200 zł. W przypadku Rady do Spraw Cyfryzacji na 18 członków z możliwości zwrotu kosztów podróży korzystają 3 osoby. Przy podobnej liczbie chętnych wchodzących w skład Rady do Spraw Ochrony Danych Osobowych roczny zwrot dojazdu dla członków wyniósłby w przybliżeniu 14000 zł. Wydatki związane z samą organizacją posiedzeń Rady do Spraw Cyfryzacji wynoszą 1280,00 zł za jedno posiedzenie (łączny roczny koszt 15 360,00 zł). **Uwzględniając powyższe, roczny koszt utrzymania Rady do Spraw Ochrony Danych Osobowych liczących 8 członków w tym przewodniczącego, wyniósłby w przybliżeniu 63 000, 00 zł.** - Projekt ustawy nakłada na Prezesa Urzędu szereg obowiązków, których realizacja możliwa jest również z wykorzystaniem systemów teleinformatycznych. Systemy takie zapewniają szybsze i bardziej efektywne egzekwowanie zasad ochrony danych osobowych oraz są wygodną formą kontaktów z organem (ze względu na elektroniczny charakter naruszeń prywatności, wyposażenie organu w środki informatyczne i elektronizacja procesu komunikacji z organem jest warunkiem koniecznym sprawnej realizacji jego obowiązków). Koszt powinien obejmować utworzenie i modyfikację systemu teleinformatycznego notyfikacji naruszeń, systemu notyfikacji danych kontaktowych inspektorów ochrony danych, systemu zarządzania dokumentacją oraz systemu rozliczeń z ukaranymi. O konieczności wprowadzenia takich systemów przesądza również kalkulacja dokonana przez Ministra Cyfryzacji. Liczba notyfikacji inspektorów ochrony danych kierowanych do Prezesa Urzędu Ochrony Danych może wynieść w przybliżeniu 390 000 notyfikacji (ok. 340 000 notyfikacji w przypadku przedsiębiorców, ok. 1 100 notyfikacji od stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej, ok. 50 000 podmiotów publicznych). Przyjmując, że w przybliżeniu liczba godzin roboczych w miesiącu wynosi 168, gdyby każda z notyfikacji spłynęła w pierwszym roku funkcjonowania Prezesa Urzędu Ochrony Danych Osobowych tj. w okresie od 25 maja 2018 r. do 25 maja 2019 r., do organu może spływać w przybliżeniu 190 notyfikacji na godzinę. Kalkulację wydajności i kosztów systemu oparto na następujących danych wejściowych: Liczba podmiotów zobowiązanych do przesłania notyfikacji wg danych GUS wynosi 393 000 rozłożonych na 2 pierwsze lata funkcjonowania organu; Na bazie statystyk naruszeń w sektorze telekomunikacyjnym szacuje się liczbę zgłoszeń naruszeń dla całej Polski na 55 000 rocznie. Okres utrzymywania danych w systemie produkcyjnym – 5 lat. Szacunkowa objętość zasobów baz danych produkcyjnych – 5 TB Szacunkowa objętość danych archiwalnych i kopii zapasowych – 15 TB Zapotrzebowanie na moc obliczeniową: Serwery baz danych i systemy plików wraz z zapewnieniem niezawodności – 2 serwery x 8 CPU x86 Serwery aplikacyjne - 4 serwery x 2 CPU x86 Serwery warstwy dostępowej 4 serwery x 2 CPU x86 Do obliczenia kosztów wykorzystano dane Gartner – największej firmy analitycznej IT, badającej i publikującej w najszerszym zakresie dane kosztowe i benchmarkingowe IT. (*Toolkit: Pricing for Data Center, Hosting and Cloud-Based Outsourcing Solutions,* 7 grudnia 2016 r., William Maurer, Mark D. Ray, Daniel Barros.) Użyto następujących danych: Średni koszt posiadania i utrzymania serwera x86 do 4 CPU 828USD miesięcznie (obejmuje sprzęt, wsparcie producenta i administrację) Średni koszt posiadania i utrzymania serwera x86 do 8 CPU 1099USD miesięcznie (obejmuje sprzęt, wsparcie producenta i administrację) Średni koszt pamięci masowej High-End Hybrid Array - 0,48 USD/miesiąc/GB Średni koszt pamięci masowej Low-End File Storage - 0,10 USD/miesiąc/GB Użyte dane dotyczą pełnego outsource'ingu infrastruktury i reprezentują łączne koszty wraz z towarzyszącym wyposażeniem, pracą administratorów, zapewnieniem ciągłości.

	W przypadku decyzji o jednorazowym zakupie infrastruktury, koszty roczne będą reprezentowały amortyzację sprzętu, wsparcie producenta i koszty wynagrodzeń, ale ich sumaryczne poziomy będą analogiczne. Dla budowy systemu gromadzenia notyfikacji i zgłoszeń przyjęto konieczność budowy systemu od zera. Założono, że jest to system w formie e-usług z pełną integracją z profilem zaufanym z zapewnieniem interoperacyjności. Przez analogię do podobnych systemów z uwzględnieniem doświadczenia Ministra Cyfryzacji złożoność systemu oceniono w drodze szacowania eksperckiego na 1 500 punktów funkcyjnych. Przyjęto nakłady na analizę i wdrożenie systemu na poziomie dwukrotności kosztów wytworzenia systemu. Przy tym oszacowaniu posłużono się danymi Gartner z raportu IT Key application measures prezentującymi koszty developmentu, jako 33 % łącznych kosztów systemu wytwarzanego w regionie europejskim. Do oszacowania kosztów budowy systemu notyfikacji na zamówienie wykorzystano dane Gartner – Key Application measures – wartość - development cost per function point - 453 USD Do przeliczenia wydatków na walutę krajową użyto średnich kursów NBP, Tabela nr 136/A/NBP/2017 z dnia 2017-07-17 1 USD =3,6767zł. Dla systemu rozliczeń przyjęto zakup systemu standardowego z półki. Cenę oprogramowania oszacowano na 450 000 zł na podstawie znanych wnioskodawcy cen zakupu średniej skali systemów ERP takich producentów jak Exact, Microsoft, Comarch dla około 50 pracowników. Ze względu na standardowość oprogramowania przyjęto koszt wdrożenia, jako równowartość oprogramowania. Dla systemu zarządzania obiegiem dokumentów przyjęto wykorzystanie systemu EZD PUW, którego licencję posiada Skarb Państwa. Na bazie doświadczeń z wdrażania tego systemu w licznych instytucjach oszacowano koszty wdrożenia na 4 etaty w ciągu 6 miesięcy. Założono, że system będzie eksploatowany na wspólnej infrastrukturze serwerowej wraz z systemem notyfikacji. Przyjęto, że infrastruktura sieciowa GIODO ani łącze internetowe nie wymaga zmiany ani rozbudowy. Do oszacowania kosztów wynagrodzeń dla utrzymania systemu wykorzystano dane z publikacji Raport płacowy Sedlak & Sedlak dla branży IT – 2016 podającej medianę wynagrodzeń podstawowych specjalistów zatrudnionych w branży IT w 2016 roku w wysokości 6 625 zł. Zapotrzebowanie na personel IT dla utrzymania systemu notyfikacji i systemu rozliczeń oceniono na 3 etaty. **Przy powyższych założeniach otrzymano oszacowanie rocznych kosztów utrzymania systemów informatycznych w przybliżeniu 2 638 360 zł. Przy czym kwota ponoszona w pierwszym roku działania organu (przez 7 miesięcy do 31 grudnia 2018 r.) wynosiła będzie proporcjonalnie w przybliżeniu 1 539 043 zł.** **Wielkość nakładów na zakup, budowę i wdrożenie systemów oszacowano w przybliżeniu na 10 951 860 zł.** - W związku z podwojeniem liczby pracowników Prezesa Urzędu, konieczne jest zwiększenie powierzchni biurowej wynajmowanej obecnie przez Generalnego Inspektora Ochrony Danych Osobowych. Przyjmując za granicę 6 m^2 wolnej powierzchni dla jednego pracownika oraz konieczność zarezerwowania przestrzeni na meble oraz urządzenia biurowe, konieczne jest przewidzenie kosztów wynajmu w przybliżeniu 1 100 m^2 dodatkowej przestrzeni biurowej. W oparciu o ocenę 15 ofert najmu powierzchni biurowej w centrum Warszawy średni miesięczny koszt wynajmu 1 m^2 wynosi 22 EURO oraz 20 zł za kosztów eksploatacyjnych. Do powyższego konieczne jest przewidzenie kosztu wynajmu powierzchni parkingowej dla floty samochodowej w kwocie 180 EURO za miejsce parkingowe miesięcznie. **Przyjmując za średni kurs EURO 4,2091 w oparciu o tabelę nr 136/A/NBP/2017 z dnia 2017-07-17, łączny roczny koszt wynajmu przestrzeni biurowej z uwzględnieniem miejsc parkingowych dla trzech pojazdów, wynosi w przybliżeniu 1 500 000 zł rocznie**. - Zwiększenie ilości zatrudnionych przez Prezesa Urzędu pracowników, a w konsekwencji zwiększenie powierzchni biurowej wiąże się z koniecznością pokrycia opłat administracyjnych obejmujących chociażby koszty sprzętu IT. Według danych Ministra Cyfryzacji łączny koszt organizacji jednego stanowiska pracy zaopatrzonego w pakiet office OnPremise oraz laptop i komputer stacjonarny to 13 800 zł, z czego koszt laptopa to koszt 5 000 zł. W przypadku 145

pracowników z zastrzeżeniem, że tylko kadra kierownicza (w przybliżeniu 30 pracowników) posiadała będzie laptopy, to w przybliżeniu koszt 1 400 000 zł.

2.1.2. Pozostałe koszty

- Koszty związane z dostosowaniem do rozporządzenia 2016/679 systemów teleinformatycznych objętych działalnością Ministra Cyfryzacji. Łączny jednorazowy koszt zmian wdrożeniowych koniecznych do podjęcia w pierwszych miesiącach rozpoczęcia stosowania rozporządzenia 2016/679 (rok „0" w tabeli wpływu regulacji na sektor finansów publicznych) oszacowany w oparciu o szczegółowe obliczenia związane z koniecznością zmiany systemów Prezesa Urzędu Ochrony Danych Osobowych podjęte w punkcie 1.1.1 przedmiotowego OSR wynosi 5 000 000 zł.

2.2. Skutki nie włączone do tabeli w związku z trudnościami z ich policzalnością

- Zmiana polegająca na nałożeniu przez rozporządzenie 2016/679 na wszystkie podmioty publiczne, o których mowa w art. 9 ustawy o finansach publicznych obowiązku wyznaczenia inspektora ochrony danych. Krajowe przepisy o ochronie danych osobowych wyłącznie doprecyzowują proceduralne aspekty informowania Prezesa Urzędu o danych kontaktowych takich inspektorów. W oparciu o informacje o liczbie podmiotów, według stanu rejestru REGON na dzień 30.06.2017 r. oraz dane z powszechnie dostępnej bazy administratorów bezpieczeństwa informacji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych wskazują, że Polsce mamy około 68 000 podmiotów publicznych, o których mowa w art. 9 ustawy o finansach publicznych. W przybliżeniu znaczna część z nich, bo około 18 000 powołało już dzisiaj administratora bezpieczeństwa informacji, koszt jego utrzymania został więc wliczony w dotychczasowych budżet działania danego podmiotu. Pozostaje więc w przybliżeniu około 50 000 podmiotów, które będą zobowiązane do powołania inspektora ochrony danych. W stosunku do nich możliwe jest jednak przyznanie takiej funkcji dotychczasowym pracownikom, co nie będzie wiązało się z kosztami po stronie żadnych jednostek. Zgodnie z art. 37 ust. 3 rozporządzenia 2016/679 *jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.* W chwili obecnej nie jest możliwe do przewidzenia ile podmiotów zdecyduje się na powołanie wspólnego Inspektora Ochrony Danych, co też znacznie obniża koszty. W związku z powyższym, wskazanie dokładnych kwot może być obciążone poważnym ryzykiem przeszacowania. Dokładna liczba podmiotów, które zdecydują się powołać taką osobę nie mając jej dotychczas w swoich zasobach nie jest więc możliwa do dokładnego wskazania.
- Przepisy rozporządzenia 2016/679 przewidują mechanizmy certyfikacji, a projekt ustawy je uzupełnia. Projekt nakłada na Prezesa Urzędu Ochrony Danych Osobowych obowiązek certyfikacji. Podejmowanie takich działań wiąże się z kosztami po stronie organu związanymi z koniecznością wypracowania kryteriów certyfikacji, udostępnienia ich za pośrednictwem Biuletynu Informacji Publicznej oraz przeprowadzenia czynności sprawdzających. Jednocześnie za czynności związane z postepowaniem o udzielenie certyfikacji Prezes Urzędu Ochrony Danych Osobowych będzie pobierał opłatę w wysokości trzykrotności przeciętnego miesięcznego wynagrodzenia za pracę w gospodarce narodowej w roku poprzednim ogłaszanego przez Prezesa Głównego Urzędu Statystycznego. Przeciętne wynagrodzenie w gospodarce narodowej w 2016 r. wyniosło 4047,21 zł, opłata za certyfikację wynosiła więc będzie 12 141,63 zł. Zgodnie z pkt. 3.2. cennika opłat za czynności związane z akredytacją Polskiego Centrum Akredytacji z dnia 18 listopada 2016 r. *za roboczodzień przyjmuje się wartość 8 godzin kalkulacyjnych PCA. Koszt jednej roboczogodziny kalkulacyjnej PCA w procesach akredytacji i nadzoru wynosi 120 zł.* W każdym przypadku na koszt takich działań składała się będzie jednak konieczność bądź brak konieczności pokrycia kosztów ewentualnych środków transportu pracowników Urzędu Ochrony Danych Osobowych, noclegów oraz dodatkowych wydatków. Opłaty powinny więc pokrywać całość wydatków poniesionych przez Prezesa Urzędu w związku z podejmowaniem czynnościami certyfikacji, a podejmowanie działań przez Prezesa Urzędu Ochrony Danych Osobowych nie powinno wiązać się z dodatkowymi wydatkami, ale podjęcie w tym zakresie dokładnych obliczeń, jest niemożliwe. Ciężko również przewidzieć, jakim zainteresowaniem będzie cieszyła się ze strony przedsiębiorców sama certyfikacja.
- Zmiana polegająca na obowiązku wnoszenia przez administrację publiczną kar finansowych za naruszenie przepisów o ochronie danych osobowych w przypadku nałożenia kary przez Prezesa

	Urzędu. Kary będą stanowiły dochód budżetu państwa, ale nie jest możliwe przewidzenie wysokości nakładanych kar. W świetle obowiązującego porządku prawnego, Generalny Inspektor Ochrony Danych Osobowych nie jest uprawniony do nakładania administracyjnych kar finansowych. - Zmiana polegająca na wnoszeniu Prezesowi Urzędu Ochrony Danych Osobowych opłat za podjęcie czynności certyfikacji przez Prezesa Urzędu. Opłaty będą stanowiły dochód budżetu państwa, ale nie jest możliwe przewidzenie ilości wnoszonych opłat a wiec certyfikacji. - Przepisy przyznają nową podstawę prawną do kierowania pozwów z tytułu naruszenia przepisów o ochronie danych osobowych do sądów powszechnych. Będzie to dla zainteresowanych równoległa (alternatywna dla drogi administracyjnej) ścieżka dochodzenia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych. Uwzględniając instancyjną strukturę polskiego sądownictwa powszechnego i nadzór judykacyjny sprawowany przez Sąd Najwyższy nad tymi sądami oraz ustanowienie nowej podstawy prawnej kierowania pozwów do tych sądów, należy spodziewać się zwiększenia liczby kierowanych do nich spraw. Będą to zupełnie nowe w praktyce sądów powszechnych sprawy o roszczenia niemajątkowe wynikające z naruszenia przepisów o ochronie danych osobowych oraz dodatkowe sprawy o roszczenia majątkowe (odszkodowania) wynikające z naruszenia w/w przepisów. Bliższe oszacowanie wielkości dodatkowego wpływu spraw do sądów powszechnych i Sądu Najwyższego spowodowanego przyjęciem projektowanych przepisów na obecnym etapie nie jest możliwe (trwają wstępne prace analityczne). Szacunek ten zostanie uzupełniony w toku dalszych prac. Z dużym prawdopodobieństwem można jednak przyjąć, że wzrost wpływu będzie wymagał wzmocnienia kadrowego sądów – dodatkowych etatów sędziowskich i urzędniczych.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa	- Przedsiębiorcy uzyskują uprawnienie do konsultowania z Prezesem Urzędu rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. - Zmiana polegająca na obowiązku wnoszenia przez przedsiębiorców administracyjnych kar finansowych za naruszenie przepisów o ochronie danych osobowych w przypadku nałożenia kary przez Prezesa Urzędu.						
	sektor mikro-, małych i średnich przedsiębiorstw	J.w.						
	rodzina, obywatele oraz gospodarstwa domowe							
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	- Zmiana polegająca na zmniejszeniu wynikających z ogólnego rozporządzenia obowiązków ciążących na podmiotach prowadzących działalność polegającą na publikowaniu materiałów prasowych. Przepisy ustawy ograniczają zastosowanie rozporządzenia unijnego względem tych podmiotów, przy czym z uwagi na szeroki zakres nowych obowiązków nałożone zostaną na nie i tak obowiązki dzisiaj nieistniejące. Z kosztami po stronie tych podmiotów wiązało się będzie realizowanie przez nie prawa do bycia zapomnianym oraz zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu i zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych. Podmioty te zobowiązane będą również do przeprowadzania oceny

	skutków projektowanych rozwiązań dla ochrony danych. Wiąże się to z kosztem dedykowania przeszkolonych pracowników do dokonania takiej oceny. W przypadku, gdy dane przetwarzane będą na szeroką skalę, konieczne będzie również wyznaczanie inspektorów ochrony danych. Uwzględniając powyższe przyjąć należy koszt po stronie takiego przedsiębiorcy w postaci dedykowania jednego pracownika, którego co najmniej połowa etatu dotyczyłaby realizacji powyższych obowiązków. W Polsce liczba podmiotów zajmujących się wydawaniem gazet oraz wydawaniem czasopism i pozostałych periodyków wynosi **3300 (lipiec 2017 r.).** Powyższa liczba przygotowana została w oparciu o dane zamieszczone w krajowym rejestrze urzędowym podmiotów gospodarki narodowej REGON. Dane zostały przygotowane z wykorzystaniem kryterium formy prawnej, formy własności, formy finasowania, działalności wg kodu PKD oraz nazwy we wskazanych przypadkach. - Zmiana polegająca na zmniejszeniu wynikających z ogólnego rozporządzenia 2016/679 obowiązków ciążących na podmiotach prowadzących działalność literacką oraz artystyczną. Przepisy ustawy ograniczają zastosowanie rozporządzenia unijnego względem tych podmiotów, przy czym z uwagi na szeroki zakres nowych obowiązków nałożone zostaną na nie i tak obowiązki dzisiaj nieistniejące. Z kosztami po stronie tych podmiotów wiązało się będzie realizowanie przez nie prawa do bycia zapomnianym oraz zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu i zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych. Podmioty te zobowiązane będą również do przeprowadzania oceny skutków projektowanych rozwiązań dla ochrony danych. Wiąże się to z kosztem dedykowania przeszkolonych pracowników do dokonania takiej oceny. W przypadku, gdy dane przetwarzane będą na szeroką skalę i nie są podmiotami publicznymi (wobec, których wymóg taki będzie ciążył zawsze), konieczne będzie również wyznaczanie inspektorów ochrony danych. Uwzględniając, że zakres gromadzonych przez takie podmioty danych jest najczęściej bardzo mały, wystarczającym wydaje się odbycie przez takie osoby stosownych szkoleń w zakresie realizacji nowych obowiązków. W Polsce liczba podmiotów zajmujących się działalnością związaną z wystawianiem przedstawień artystycznych, działalnością wspomagająca wystawianie przedstawień artystycznych, artystyczną i literacką działalnością twórczą oraz działalnością obiektów kulturalnych wynosi **20 071 (lipiec 2017 r.).** Powyższa liczba przygotowana została w oparciu o dane zamieszczone w krajowym rejestrze urzędowym podmiotów gospodarki narodowej REGON. Dane zostały przygotowane z wykorzystaniem kryterium formy prawnej, formy własności, formy finasowania, działalności wg kodu PKD oraz nazwy we wskazanych przypadkach. - **Zmiana polegająca na nałożeniu na przedsiębiorców powołujących inspektorów ochrony danych do ich notyfikacji** do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku przedsiębiorców, których główna działalność polega na regularnym i systematycznym monitorowaniu osób, których dane dotyczą, na dużą skalę lub główna działalność polega na przetwarzaniu danych szczególnie chronionych na dużą skalę oraz danych dotyczących skazań. Grupa Robocza art. 29 jako unijne forum współpracy organów ochrony danych osobowych w wytycznych dotyczących inspektorów ochrony danych ('DPO')(16/EN WP 243 rew.01) wskazała, że wymóg wyznaczenia inspektora ochrony danych dotyczył będzie przedsiębiorców zajmujących się obsługą sieci telekomunikacyjnej, świadczeniem usług telekomunikacyjnych, przekierowywaniem poczty elektronicznej, działaniami marketingowymi opartymi na danych, profilowaniem i ocenianiem dla celów oceny ryzyka (na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy), śledzeniem lokalizacji, na przykład przez aplikacje mobilne, programy lojalnościowe, reklamą behawioralną, monitorowaniem danych dotyczących zdrowia i kondycji fizycznej za pośrednictwem urządzeń przenośnych, monitoringiem wizyjnym, urządzeniami skomunikowanymi np. inteligentne liczniki, inteligentne samochody, automatyka domowa. Bez wątpienia podmiotami takimi będą również operatorzy medyczni przetwarzający dane osobowe szczególnie chronione dotyczące stanu zdrowia. Ilość podmiotów wykonujących działalność leczniczą na dzień 11 lipca 2017 r. znajdujących się w Rejestrze Podmiotów Wykonujących Działalność Leczniczą wynosi **21 438** podmiotów, z czego podmiotów niepublicznych (wynik w oparciu o kryterium wyszukiwania w bazie z wykorzystaniem zwrotu „Publiczny" pojawiający się w nazwie podmiotu) ok. **700** podmiotów. Zdecydowana większość podmiotów to podmioty niepubliczne. Liczba przedsiębiorców telekomunikacyjnych na dzień 11 lipca 2017 r. znajdujących się w Rejestrze Przedsiębiorców Telekomunikacyjnych wynosi 6 023 podmiotów. Rejestr Usług Płatniczych na dzień 11 lipca 2017 r. wynosi 12 936 podmiotów. W przybliżeniu ilość podmiotów wyłącznie w wybranych branżach przekracza **40 000** podmiotów. Powyższe stanowi wyłącznie 1,16 % wszystkich przedsiębiorców według stanu rejestru REGON na dzień 30.06.2017 r. Uwzględniając powołaną opinię Grupy Roboczej art. 29 uznającą za okoliczność

	wystarczającą do nałożenia na przedsiębiorcę obowiązku powołania inspektora ochrony danych podejmowanie przez niego działań marketingowych opartych na danych, procent takich przedsiębiorców należy zwiększyć co najmniej 10 krotnie. W świetle powyższego w przybliżeniu 342 700 przedsiębiorców zobowiązana byłaby do powołania inspektora ochrony danych. Znaczna część z nich zmuszona będzie do powołania inspektora ochrony danych nie mając obecnie w swojej organizacji osoby podejmującej takie działania. W rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych na dzień 11 lipca 2017 r. znajdowało się bowiem tylko 25 316 osób pełniących funkcję administratora bezpieczeństwa informacji, z czego znaczna część powołana została przez administrację publiczną. - Zmiana polegająca na nałożeniu na stowarzyszenia, inne organizacje społeczne i zawodowe, fundacje oraz samodzielne publiczne zakłady opieki zdrowotnej powołujących inspektorów ochrony danych obowiązku ich notyfikacji do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku gdy ich główna działalność polega na regularnym i systematycznym monitorowaniu osób, których dane dotyczą, na dużą skalę lub główna działalność polega na przetwarzaniu danych szczególnie chronionych na dużą skalę oraz danych dotyczących skazań. Informacje o liczbie podmiotów, według stanu rejestru REGON na dzień 30.06.2017 r. wskazują, że w Polsce liczba takich podmiotów wynosi **110 010**. **Przyjmując, że obowiązek powołania inspektora ochrony danych ciążył będzie wyłącznie na 1 % podmiotów to obejmie on 1 100 podmiotów.**

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☐ nie dotyczy
☒ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☒ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:

- Rozporządzeniem 2016/670 oraz projektem ustawy o ochronie danych osobowych wprowadzony zostaje obowiązek notyfikacji organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych) danych kontaktowych inspektorów ochrony danych, którzy zastąpią dzisiejszych administratorów bezpieczeństwa informacji. Obowiązek obciąża zarówno przedsiębiorców jak i organy administracji publicznej, jako dokonujących notyfikacji, jak i Prezesa Urzędu Ochrony Danych Osobowych jako otrzymującego takie notyfikacje.
- Założeniem projektu ustawy o ochronie danych osobowych jest skrócenie czasu postępowań prowadzonych w sprawach naruszeń przepisów o ochronie danych osobowych poprzez wskazanie maksymalnego terminu na przeprowadzenie postępowania kontrolnego (30 dni) oraz zniesienie dwuinstancyjności postępowania w sprawach naruszeń.
- Projekt ustaw nie przewiduje istniejącego dotychczas obowiązku rejestracji zbiorów danych osobowych oraz administratorów bezpieczeństwa informacji. Organ nadzorczy nie będzie również zobowiązany do prowadzenia rejestrów zbiorów danych osobowych oraz administratorów bezpieczeństwa informacji. Przepisy nakładają na podmioty sektora publicznego oraz znaczną część podmiotów prywatnych wymóg powołania i notyfikacji inspektorów ochrony danych.
- Projekt wymusza wprowadzenie w Urzędzie Ochrony Danych Osobowych systemów telekomunikacyjnych ułatwiających rozpatrywanie przez organ spraw, otrzymywanie notyfikacji oraz utrzymywanie kontaktu z obywatelami.
- Projekt ustawy o ochronie danych osobowych wprowadza nowe procedury w zakresie notyfikacji inspektorów ochrony danych, notyfikacji naruszeń przepisów o ochronie danych osobowych, certyfikacji, dochodzenia roszczeń cywilnoprawnych z tytułu naruszenia przepisów o ochronie danych osobowych.
- Rozporządzenie 2016/670 oraz projekt ustawy o ochronie danych osobowych znosi ogólny obowiązek dokumentacyjny w zakresie ochrony danych osobowych. Został on zastąpiony zasadą rozliczalności.

9. Wpływ na rynek pracy

Projekt przepisów ustawy o ochronie danych osobowych będzie pozytywnie wpływał na rynek pracy. Przepisy nakładają na podmioty sektora publicznego oraz znaczną część podmiotów prywatnych wymóg powołania i notyfikacji inspektorów ochrony danych. Stanowisku takiemu odpowiada funkcja dzisiejszego administratora bezpieczeństwa informacji. Uwzględniając powyższe oraz fakt, że w dzisiejszym rejestrze Administratorów Bezpieczeństwa Informacji

zarejestrowanych jest jedynie 25 357 osób, na rynku pracy pojawi się znaczna liczba nowych miejsc pracy. Na zwiększenie liczby miejsc pracy wpłynie również zwiększenie liczby etatów w Urzędzie Ochrony Danych Osobowych.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☒ inne: Wolności i prawa obywateli	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	- Rozporządzenie 2016/679 oraz projekt ustawy o ochronie danych osobowych wymusza wprowadzenie w Urzędzie Ochrony Danych Osobowych systemów telekomunikacyjnych ułatwiających rozpatrywanie przez organ spraw, otrzymywanie notyfikacji oraz utrzymywanie kontaktu z obywatelami. Zmiany wymuszają również dostosowanie systemów teleinformatycznych do nowych przepisów o ochronie danych osobowych.

11. Planowane wykonanie przepisów aktu prawnego

W dniu 4 maja 2016 r. w Dzienniku Urzędowym UE L 119 zostało opublikowane 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. Zgodnie z art. 99 ogólnego rozporządzenia o ochronie danych, rozporządzenie wchodzi w życie 20 dnia po publikacji w Dzienniku Urzędowym UE. Rozporządzenie 2016/679 będzie bezpośrednio obowiązujące, skuteczne oraz stosowane od 25 maja 2018 r. i tym dniu powinny zacząć obowiązywać krajowe przepisy zapewniające skuteczne stosowanie rozporządzenia 2016/679 w polskiej przestrzeni prawnej.
Minister Cyfryzacji przewiduje prowadzenie działań zmierzających do zwiększania świadomości społecznej w przedmiocie zmiany przepisów o ochronie danych osobowych, w tym poprzez udział pracowników Ministerstwa w licznych konferencjach oraz przekazach prasowych.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

- Projekt ustawy o ochronie danych osobowych nakłada na Prezesa Urzędu Ochrony Danych Osobowych obowiązek przedstawiania sprawozdania właściwym organom administracji publicznej. Sprawozdanie zawierało będzie 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. Sprawozdanie za dany rok kalendarzowy będzie składane do dnia 30 czerwca roku następnego i będzie stanowiło ważne źródło informacji o zakresie działań podejmowanych przez Prezesa Urzędu.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Rozporządzenie 2016/679:
http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.POL&toc=OJ:L:2016:119:TOC
Ocena skutków rozporządzenia 2016/679:
http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf
Dokładna kalkulacje w zakresie Oceny Skutków Regulacji w ustawie o ochronie zabytków i opieki nad zabytkami - EXCEL