SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Prezes Rady Ministrów
RM-10-49-18

Druk nr 2410

Warszawa, 5 kwietnia 2018 r.

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o ochronie danych osobowych

z projektami aktów wykonawczych.

Projekt ma na celu wykonanie prawa Unii Europejskiej.

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

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

Z poważaniem

(-) Mateusz Morawiecki

Projekt

U S T A W A

z dnia

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

---

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

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

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

Rozdział 1

Przepisy ogólne

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

2. Ustawa określa:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Postępowanie przed Prezesem Urzędu jest postępowaniem jednoinstancyjnym.

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

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

Rozdział 2

Wyznaczanie inspektora ochrony danych

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 3

Warunki i tryb udzielania akredytacji podmiotowi certyfikującemu

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

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

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

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

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

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

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

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

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

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

Rozdział 4

Warunki i tryb dokonywania certyfikacji

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Certyfikat zawiera co najmniej:

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

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

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

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

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

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

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

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

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

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

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

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

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

1) imię i nazwisko osoby przeprowadzającej czynności sprawdzające;

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

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

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

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

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

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

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

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

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

5. Opłata stanowi dochód budżetu państwa.

Rozdział 5

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Certyfikat akredytacyjny zawiera co najmniej:

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

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

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

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

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

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

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

Rozdział 6

Prezes Urzędu Ochrony Danych Osobowych

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
6) posiada nieposzlakowaną opinię.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Do zadań Rady należy:

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

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

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

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

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

6. Rada składa się z 8 członków.

7. Kandydatów na członków Rady zgłasza:

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

8. Członkiem Rady może być osoba, która:

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

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

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

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

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

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

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

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

15. Obsługę Rady zapewnia Urząd.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Art. 55. 1. Prezes Urzędu:

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

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

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

Art. 57. Prezes Urzędu, w drodze decyzji:

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

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

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

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

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

Rozdział 7

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Na postanowienie przysługuje skarga do sądu administracyjnego.

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

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

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

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

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

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

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

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

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

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

9. Sąd sporządza uzasadnienie postanowienia w terminie 21 dni.

10. Od wniosku nie pobiera się opłaty sądowej.

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

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

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

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

Rozdział 8

Europejska współpraca administracyjna

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

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

3. Na postanowienie przysługuje skarga do sądu administracyjnego.

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

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

Rozdział 9

Kontrola przestrzegania przepisów o ochronie danych osobowych

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

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

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

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

– zwany dalej „kontrolującym”.

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

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

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

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

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

4. O wyłączeniu kontrolującego rozstrzyga Prezes Urzędu.

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

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

2. Imienne upoważnienie do przeprowadzenia kontroli zawiera:

1) wskazanie podstawy prawnej przeprowadzenia kontroli;
2) oznaczenie organu;

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

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

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

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

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

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

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

Art. 84. 1. Kontrolujący ma prawo:

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

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

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

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

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

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

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

okazaniu upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej kontrolującego.

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

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

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

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

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

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

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

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

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

2. Protokół kontroli zawiera:

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 10

Odpowiedzialność cywilna i postępowanie przed sądem

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 11

Przepisy o administracyjnych karach pieniężnych i przepisy karne

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

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

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

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

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

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

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

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

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

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

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

3. Do wniosku dołącza się uzasadnienie.

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 12

Przepisy zmieniające

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

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

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

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

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

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

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

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

1) użyte w art. 4 w ust. 1 i 2 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych” zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych”;
2) w art. 29 w ust. 1 w pkt 2 lit. i otrzymuje brzmienie:

„i) przetwarzania danych osobowych, z wyjątkiem danych ujawniających poglądy polityczne, przekonania religijne lub światopoglądowe, jak również danych genetycznych, o nałogach, o seksualności lub o orientacji seksualnej.”.

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

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

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

---

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

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

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

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

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

1) w art. 14 § 4 otrzymuje brzmienie:

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1) w art. 13 § 5 otrzymuje brzmienie:

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

2) w art. 191 uchyla się § 2.

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 13

Przepisy przejściowe i dostosowujące

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 14

Przepisy końcowe

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

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

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

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

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

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

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

UZASADNIENIE

Opracowanie projektu nowej ustawy o ochronie danych osobowych wynika z konieczności zapewnienia stosowania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „Rozporządzeniem".

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

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

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

Rozdział 1 Przepisy ogólne

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

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

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

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

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

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

1) w ramach działalności nieobjętej zakresem prawa Unii;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

– wypowiedzi w ramach działalności literackiej,

– wypowiedzi w ramach działalności artystycznej,

– wypowiedzi akademickiej.

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

Wyłączono zatem następujące obowiązki administratora lub podmiotu przetwarzającego:

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

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

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

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

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

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

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

– art. 5 – zasady przetwarzania danych osobowych,

– art. 6 – przesłanki legalności przetwarzania danych osobowych,

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

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

– art. 9 – przetwarzanie szczególnych kategorii danych,

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

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

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

– art. 16 – prawo do sprostowania danych,

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

– art. 20 – prawo do przenoszenia danych,

– art. 21 – prawo do sprzeciwu,

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

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

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

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

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

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

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

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

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

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

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

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

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

1) zmiana celu przetwarzania służy realizacji zadania publicznego;

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

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

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

   b) naruszy ochronę informacji niejawnych.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

zachowanie dodatkowych warunków bezstronności zasad dokonywania certyfikacji przez Prezesa Urzędu.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 14. Przepisy przejściowe i dostosowujące.

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

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

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

Rozdział 15. Przepisy końcowe.

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

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

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

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

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

Projekt nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

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

Nazwa projektu Projekt ustawy o ochronie danych osobowych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Marek Zagórski – Sekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Dr Maciej Kawecki, Dyrektor Departamentu Zarządzania Danymi w Ministerstwie Cyfryzacji maciej.kawecki@mc.gov.pl	**Data sporządzenia** 27.03.2018 r. **Źródło:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE **Nr w wykazie prac UC 101**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W dniu 25 maja 2016 r. weszło w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: rozporządzenie 2016/679). Ministerstwo Cyfryzacji jest resortem odpowiedzialnym za zapewnienie skutecznego stosowania rozporządzenia w polskiej przestrzeni prawnej przez przyjęcie właściwej ustawy krajowej zastępującej obowiązującą obecnie ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922), dalej: „ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych", oraz zmianę właściwych przepisów sektorowych. Organem właściwym do przygotowania nowej regulacji prawnej w zakresie ochrony danych osobowych jest minister właściwy do spraw informatyzacji, gdyż do jego zadań, zgodnie z art. 12a ust. 1 pkt 8 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2016 r., poz. 2260, z późn. zm.) należą sprawy kształtowania polityki państwa w zakresie ochrony danych osobowych. **Rozporządzenie 2016/679 zacznie być aktem bezpośrednio stosowanym oraz bezpośrednio skutecznym 25 maja 2018 r. i do tego czasu każde z państw członkowskich zobowiązane jest do zapewnienia jego skutecznego stosowania w swoim porządku prawnym poprzez przyjęcie właściwych przepisów wewnętrznych.** W ramach realizacji tej kompetencji Minister Cyfryzacji przygotował projekt nowej ustawy o ochronie danych osobowych oraz zmian w przepisach sektorowych wprowadzanych projektem ustawy wprowadzającej ustawę o ochronie danych osobowych. Podjęte działania legislacyjne zgodnie z zasadami prawa Unii Europejskiej opierały się na założeniu, że nowa ustawa o ochronie danych osobowych będzie zawierała wyłącznie przepisy, które zostały przez prawodawcę unijnego wprost przekazane do uregulowania w prawie krajowym, oraz takie, w których rozporządzenie 2016/679 pozostawiło pewną swobodę regulacyjną poszczególnym państwom członkowskim. W szczególności przedmiotem nowej ustawy o ochronie danych osobowych są kwestie dotyczące krajowego organu nadzorczego, postępowania przed tym organem, postępowania kontrolnego, wieku dziecka wymaganego do samodzielnego wyrażania zgody na przetwarzanie danych osobowych w odniesieniu do usług społeczeństwa informacyjnego, certyfikacji, sądowej ochrony praw przysługujących. Jednym z zagadnień, które musi być rozwiązane w związku z reformą systemu ochrony danych osobowych, jest zapewnienie efektywniejszego od obowiązującego obecnie systemu ochrony danych osobowych. Według informacji uzyskanych przez Ministra Cyfryzacji w związku z analizą wyroków wydawanych przez Naczelny Sąd Administracyjny w 2015 r. spośród spraw, które trafiły do sądów, średni czas trwania postępowania w sprawach dotyczących zasad naruszenia ochrony danych osobowych w Polsce wynosi 295 dni do czasu wydania przez Generalnego Inspektora Ochrony Danych Osobowych decyzji w I instancji, a do decyzji w II instancji – 437 dni. Nie lepiej jest w momencie, gdy czeka się na uzyskanie prawomocnego orzeczenia w sprawie dot. ochrony danych osobowych. Tutaj zainteresowany czeka średnio 600 dni. Wskazane statystyki pokazują ogromną skalę problemu, z którą mamy do czynienia. W 2015 r. prowadzone były postępowania (takimi statystykami dysponujemy), gdy obywatel do czasu uzyskania prawomocnego wyroku w sprawie czekał ponad 1600 dni, a więc ponad 4 lata. Założeniem przyświecającym Ministrowi Cyfryzacji w zapewnieniu skutecznego stosowania rozporządzenia 2016/679 w polskiej przestrzeni prawnej jest przyśpieszenie trwających postępowań poprzez utrzymanie terminów wynikających z ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257); zasadą jest wydanie rozstrzygnięcia niezwłocznie. W swoim piśmie z dnia 26 czerwca 2017 r. do Generalnego Inspektora Ochrony Danych Osobowych Rzecznik Praw Obywatelskich wskazał, że *do Biura Rzecznika Praw Obywatelskich napływają regularne skargi, w których obywatele wskazują na opieszałość organu ochrony danych osobowych, długotrwałe rozpoznawanie spraw i kilkuletnie oczekiwanie na wydanie decyzji przez GIODO. O konkretnych indywidualnych sprawach RPO informuje Biuro GIODO w trybie ustawy o RPO, prosząc na bieżąco o informacje i wyjaśnienia. Obywatele mają bowiem prawo oczekiwać, że ich sprawy będą rozpatrywane bez zbędnej zwłoki, zgodnie z kpa.* Na podobne problemy w funkcjonowaniu polskiego systemu ochrony danych osobowych uwagę wskazywała również Helsińska Fundacja Praw Człowieka w swoim raporcie dotyczącym mechanizmów dochodzenia ochrony w zakresie danych osobowych w Polsce**.** Sam Generalny Inspektor Ochrony Danych Osobowych na swojej stronie internetowej udostępnił komunikat, w którym

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 Europejskiej;
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. Uregulowano tryb notyfikacji inspektorów ochrony danych osobowych oraz podmioty obowiązane w polskim porządku prawnym do wyznaczenia inspektora ochrony danych osobowych.
3. Uregulowano zasady certyfikacji oraz tryb postępowania w tych sprawach. W projekcie ustawy zaproponowano, aby w polskim systemie prawnym certyfikacji udzielał organ nadzorczy, a więc Prezes Urzędu Ochrony Danych Osobowych oraz podmioty certyfikujące, wg kryteriów określonych przez Prezesa Urzędu, z uwzględnieniem art. 43 ust. 2 rozporządzenia 2016/679, i opublikowanych w Biuletynie Informacji Publicznej.
4. 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 uchylającej decyzję ramową Rady 2008/977/WSiSW.
5. 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 dwuinstancyjność 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.
6. 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, aby 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.

7. 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.

8. 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).

9. 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. 102 postanowił, że kary mogą być nakładane na podmioty wymienione w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych oraz na Narodowy Bank Polski i instytuty badawcze, a ich wysokość nie może przekroczyć 100 000 zł. Natomiast w odniesieniu do podmiotów wskazanych w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych wysokość kary nie może przekroczyć 10 000 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 wszystkich 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 planowało 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 niebędących 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.
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

[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.

			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, nieistniejących 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 sądów 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. - Rozpatrywanie wniosków Prezesa Urzędu o zadanie pytania prawnego do TSUE.
Polskie Centrum Akredytacji	1		- Rozszerzenie zakresu działalności PCA w obszarze akredytacji podmiotów dokonujących certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679.

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, aby 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 2018 r. 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 zostały 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 były 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 zostały również na stronie internetowej Ministerstwa Cyfryzacji oraz na platformie internetowej służącej konsultacjom publicznym www.konsultacje.gov.pl.

W dniu 14 września 2017 r. Minister Cyfryzacji wystosował zaproszenie do zaopiniowania projektu – było ono wysłane bezpośrednio na adresy e-mail do organizacji społecznych, związków pracodawców i stowarzyszeń branżowych w łącznej liczbie 189 podmiotów.
Równolegle informacja o rozpoczęciu konsultacji społecznych (wraz z projektem ustawy w wersji z dnia 13.09.2017 r.) ukazała się na stronie internetowej Ministerstwa Cyfryzacji www.mc.gov.pl (zakładka konsultacje społeczne) i zaproszenie do udziału w nich było szeroko dystrybuowany w mediach społecznościowych (statystyki dostępne pod linkiem: http://blog.mc.gov.pl/?p=153). Dla potrzeb przyjmowania uwag w domenie mc.gov.pl stworzono dedykowany projektowi adres e-mail: konsultacje.odo@mc.gov.pl
W toku konsultacji społecznych, trwających do 13 października 2017 r., opinie do ustawy zgłosiło ponad 110 organizacji i obywateli, którzy zgłosili w sumie 641 uwag (tabela z ich zestawieniem jest dostępna na stronie: http://legislacja.rcl.gov.pl/projekt/12302950

W ramach opiniowania projekt ustawy został przekazany Komisji Wspólnej Rządu i Samorządu Terytorialnego. Komisja Wspólna Rządu i Samorządu Terytorialnego pozytywnie zaopiniowała projektowaną ustawę.

Projekt w ramach konsultacji został przesłany Radzie Dialogu Społecznego i do reprezentatywnych związków zawodowych oraz organizacji przedsiębiorców.

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	**2,46**	**4,36**	**4,47**	**4,47**	**4,47**	**4,47**	**4,47**	**4,47**	**4,47**	**4,47**	**4,47**	**47,05**
budżet państwa	0,57	0,97	0,97	0,97	0,97	0,97	0,97	0,97	0,97	0,97	0,97	**10,27**
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**
Fundusz Ubezpieczeń Społecznych	1,34	2,41	2,49	2,49	2,49	2,49	2,49	2,49	2,49	2,49	2,49	**26,16**
Fundusz Pracy	0,21	0,37	0,38	0,38	0,38	0,38	0,38	0,38	0,38	0,38	0,38	**4,00**
Narodowy Fundusz Zdrowia	0,34	0,61	0,63	0,63	0,63	0,63	0,63	0,63	0,63	0,63	0,63	**6,62**
Wydatki ogółem	**19,64**	**13,54**	**13,90**	**13,90**	**13,90**	**13,90**	**13,90**	**13,90**	**13,90**	**13,90**	**13,90**	**158,28**
budżet państwa	19,64	13,54	13,90	13,90	13,90	13,90	13,90	13,90	13,90	13,90	13,90	158,28

JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	**-17,18**	**-9,18**	**-9,43**	**-9,43**	**-9,43**	**-9,43**	**-9,43**	**-9,43**	**-9,43**	**-9,43**	**-9,43**	**-111,23**
budżet państwa	-19,07	-12,57	-12,93	-12,93	-12,93	-12,93	-12,93	-12,93	-12,93	-12,93	-12,93	**-148,01**
JST												
pozostałe jednostki (oddzielnie)												
Fundusz Ubezpieczeń Społecznych	1,34	2,41	2,49	2,49	2,49	2,49	2,49	2,49	2,49	2,49	2,49	**26,16**
Fundusz Pracy	0,21	0,37	0,38	0,38	0,38	0,38	0,38	0,38	0,38	0,38	0,38	**4,00**
Narodowy Fundusz Zdrowia	0,34	0,61	0,63	0,63	0,63	0,63	0,63	0,63	0,63	0,63	0,63	**6,62**

Źródła finansowania	Wydatki budżetu państwa (część 27 – Informatyzacja, budżet Polskiego Centrum Akredytacji) będą ponoszone bez konieczności dodatkowego zwiększania limitów. Wydatki w części 10 - Generalny Inspektor Danych Osobowych zostaną zwiększone w 2018 r. w ramach środków z rezerwy celowej poz. 73 - Rezerwa na zmiany systemowe i niektóre zmiany organizacyjne, w tym nowe zadania oraz na zadania związane z poprawą finansów publicznych, w tym odbudową dochodów budżetu państwa. Wejście w życie projektowanej regulacji nie będzie podstawą do ubiegania się o dodatkowe środki z budżetu państwa na ten cel.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	**Skutki przewidziane w tabeli w okresie 10 lat od wejścia w życie zmian** **1.Koszty związane z funkcjonowaniem Prezesa Urzędu Ochrony Danych Osobowych - część budżetu państwa 10 – Generalny Inspektor Danych Osobowych.** **Wysokość wydatków związanych z wejściem w życie projektowanej ustawy wyniesie w roku 2018 ok. 19 639 000 zł, w tym koszty wynagrodzeń, utrzymania systemu, wynajmu powierzchni oszacowano za okres od czerwca do grudnia 2018 r.** Na ww. wydatki składa się: **a) koszt wymiany tablicy emaliowanej z nazwą urzędu, który w przybliżeniu wyniesie 25 810,00 zł, przy uwzględnieniu wskazanej poniżej konieczności zatrudnienia w Urzędzie Ochrony Danych Osobowych dodatkowych 100 osób**. Koszt wymiany tablicy emaliowanej z nazwą urzędu to w przybliżeniu 770 zł, koszt zmiany nazwy wewnętrznej tablicy informacyjnej w przybliżeniu 540 zł, wymiana 5 szt. metalowych pieczęci urzędowych w przybliżeniu 2500 zł, wykonanie nowych obwolut na dokumenty w przybliżeniu 2500 zł, zakup materiałów promocyjnych 3500 zł, koszt nowej pieczątki + wizytówek dla wszystkich pracowników – ok 160 zł/os. **b) wysokość wynagrodzeń wraz z pochodnymi w związku z zatrudnieniem dodatkowych 100 etatów, który wyniesie ok. 5 190,00 tys. zł, a w roku 2019 r. ok. 9 339,00, natomiast w latach następnych ok. 9 654,00 tys. zł. (w latach 2019–2028 uwzględniono również dodatkowe wynagrodzenie roczne tzw. „13" – w roku 2019 za okres 7 miesięcy roku poprzedniego).** Do oszacowania ww. wydatków przyjęto poniżej przedstawione założenia. 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, nieistniejących w obowiązującym stanie prawnym obowiązków. Powyższe wydatki zostały oszacowane w oparciu o dane zawarte w sprawozdaniu Generalnego Inspektora z 2016 r., opublikowanego na stronie internetowej GIODO, gdzie liczba pracowników na dzień 31 grudnia 2016 r. wyniosła 151,525 etatu, budżet na wynagrodzenia 11 287,00 zł oraz pochodne od wynagrodzeń 2 194,00 zł. 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 ze zwiększeniem liczby 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 2016 r. wynika, że otrzymał on w 2016 r. 163 takie notyfikacje. Liczba przedsiębiorców telekomunikacyjnych na dzień 11 lipca 2017 r. znajdujących się w Rejestrze Przedsiębiorców Telekomunikacyjnych wynosi 6023 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 4600 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. Powyższe informacje nie obejmują 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. **c) koszt utrzymania Rady do Spraw Ochrony Danych Osobowych oraz wydatki na wynagrodzenia 8 członków w tym przewodniczącego, który wyniósłby w roku 2018 w przybliżeniu 37 077,00 zł, a w latach następnych 63 560,00 zł.** Do oszacowania ww. wydatków przyjęto poniżej przedstawione założenia. 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 miesiącu, łączny roczny koszt wynagrodzeń jej 8 członków wyniósłby 34 200,00 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 14 000,00 zł. Wydatki związane z samą organizacją posiedzeń Rady do Spraw Cyfryzacji wynoszą 1 280,00 zł za jedno posiedzenie (łączny roczny koszt 15 360,00 zł). **d) koszt utrzymania systemów informatycznych, który rocznie w przybliżeniu wyniesie 2 638 360,00 zł. Przy czym kwota ponoszona w pierwszym roku działania organu (przez 7 miesięcy do 31 grudnia 2018 r.) wynosiła będzie proporcjonalnie w przybliżeniu 1 539 043,00 zł. Wielkość nakładów w 2018 roku na zakup, budowę i wdrożenie systemów oszacowano w przybliżeniu na 10 951 860,00 zł.** Do oszacowania ww. wydatków przyjęto poniżej przedstawione wyjaśnienia. 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 1500 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 r. w wysokości 6 625 zł.

e) koszt wynajmu przestrzeni biurowej z uwzględnieniem miejsc parkingowych dla trzech pojazdów, który wyniesie w roku 2018 – 875 000,00 zł, a w latach następnych w przybliżeniu 1 500 000,00 zł rocznie (przyjmując za średni kurs EURO 4,2091 w oparciu o tabelę nr 136/A/NBP/2017 z dnia 2017-07-17).
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 1100 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 kosztów eksploatacyjnych. Do powyższego konieczne jest przewidzenie kosztu wynajmu powierzchni parkingowej dla floty samochodowej w kwocie 180 EURO za miejsce parkingowe miesięcznie.

f) koszt organizacji jednego stanowiska pracy zaopatrzonego w pakiet office OnPremise i komputer stacjonarny, który wyniesie 10 200,00 zł. Łącznie koszt utworzenia stanowisk pracy dla 100 etatów wyniesie 1 020 000,00 zł.
Zwiększenie ilości zatrudnionych przez Prezesa Urzędu pracowników wiąże się z koniecznością kosztów obejmujących zakup: wyposażenia i sprzętu IT (koszt jednostkowy to 9 000,00 zł) oraz licencji Microsoft Office Professional 2016 (koszt jednostkowy 1 200,00 zł).

2. Wydatki części budżetu państwa 27 – Informatyzacja, w kwocie łącznej 5 000 000,00 zł, na którą składa się jednorazowy koszt zmian wdrożeniowych koniecznych do podjęcia w pierwszych miesiącach rozpoczęcia stosowania rozporządzenia 2016/679 związany z koniecznością zmiany systemów, zostaną sfinansowane w 2018 roku w ramach dotychczasowego limitu wydatków tej części budżetowej i nie będą stanowić podstawy do ubiegania się o przyznanie dodatkowych środków z budżetu państwa.
Wskazane powyżej koszty to koszty związane z dostosowaniem do rozporządzenia 2016/679 systemów teleinformatycznych utrzymywanych przez Ministra Cyfryzacji tj.- SRP, CEPiK, ePUAP/PZ, obywatel.gov.pl, system EZD /PUW, mDkumenty. Art. 32 ww. rozporządzenia nakłada na każdego administratora danych obowiązek dokonania oceny ryzyka związanego z przetwarzaniem danych osobowych oraz wdrożenia adekwatnych systemów zabezpieczających dane – nie wskazując jednocześnie, jakim wymogom technicznym systemy takie powinny podlegać. Z kolei zgodnie z art. 20 tegoż rozporządzenia każda osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego wszystkie dane osobowe jej dotyczące, przetwarzane w systemach administratora oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Powyższe wymusza na resorcie cyfryzacji dokonanie daleko idących zmian systemów informatycznych.

3. Wydatki budżetu Polskiego Centrum Akredytacji, w kwocie łącznej 1 115 tys. zł, na którą składają się wydatki na wynagrodzenia ok. 100 tys. zł rocznie, koszt utworzenia stanowiska pracy, szkolenia pracownika ok. 15 tys., zostaną poniesione w ramach osiągniętych przychodów.
Rozszerzenie zakresu działalności PCA w obszarze akredytacji podmiotów dokonujących certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, na rzecz przedmiotu projektowanej ustawy wiąże się z koniecznością opracowania, a następnie nadzorowania specyficznego programu akredytacji, co wiąże się ze zwiększeniem zatrudnienia w PCA o 1 specjalistę-eksperta do działu akredytacji (dla przewidywanej liczby akredytowanych podmiotów ok. 20). Roczny koszt wynagrodzenia określony na podstawie zasad wynagradzania pracowników PCA oszacowano na kwotę 100 tys. zł. Do tego należy doliczyć koszty związane z utworzeniem stanowiska pracy i szkoleniem pracownika (koszt w pierwszym roku ok. 15 tys.)
Potrzeba zwiększenia zatrudnienia wynika między innymi z konieczności opracowania i uzgodnienia z zainteresowanymi stronami programu akredytacji, jego wdrożenia do stosowania w działalności akredytacyjnej PCA, przeszkolenia auditorów prowadzących oceny w przedmiotowym obszarze, a w kolejnych latach – utrzymania aktualności programu akredytacji, monitorowania i harmonizacji działań auditorów oraz corocznego nadzorowania z poziomu

PCA działalności akredytowanych jednostek certyfikujących. Jednocześnie należy stwierdzić, że PCA pobierając opłaty za czynności związane z akredytacją uzyska zwiększone przychody z tytułu akredytacji jednostek certyfikujących. Szacunkowy przewidywany dochód PCA z tytułu akredytacji / rozszerzenia akredytacji już funkcjonujących akredytowanych jednostek w pierwszym roku funkcjonowania programu wyniesie ok. 120 tys. zł (dla przewidywanej liczby 20 akredytowanych jednostek). Natomiast w kolejnych latach nadzoru nad akredytowanymi jednostkami dochód z tego tytułu będzie wynosił ok. 95 tys. zł. W rezultacie dochody PCA z tytułu rozszerzenia działalności akredytacyjnej w obszarze oceny zgodności właściwej dla projektowanej ustawy w praktyce pokryją koszty zwiększonego zatrudnienia i jednocześnie zapewnią funkcjonowanie PCA na zasadzie jednostki non-profit. Ewentualne zmiany w zakresie kosztów zatrudnionego pracownika i dochodów z tytułu rozszerzonej działalności akredytacyjnej PCA pokryje z pozostałych przychodów z tytułu akredytacji. Zwiększenie zatrudnienia w PCA o 1 pracownika nie obciąży budżetu państwa.

4. Skutki niewłączone 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 w 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, powołała już dzisiaj administratora bezpieczeństwa informacji, koszt jego utrzymania został więc wliczony w dotychczasowy 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.

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 więc 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, gdyż wcześniej nie istniała podstawa prawna do kierowania pozwów z tytułu naruszenia przepisów o ochronie danych osobowych.

5. Dochody budżetu państwa

Dochody budżetu państwa w roku 2018 wyniosą w przybliżeniu 566 609,19 zł z tytułu opłaty za certyfikację, przy maksymalnej ilości certyfikatów wydawanych przez Prezesa Urzędu, natomiast w latach następnych kwota dochodów nie przekroczy 971 330,04 zł. Do oszacowania dochodów budżetu państwa przyjęto poniżej przedstawione założenia.

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 postępowaniem o udzielenie certyfikacji Prezes Urzędu Ochrony Danych Osobowych będzie pobierał opłatę w wysokości czterokrotności 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 16 188,84 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.* Przy założeniu, że do tej pory jednostki akredytujące wydawały rocznie około 44 certyfikaty, przy czym certyfikaty przewidziane w RODO mają szerszy wymiar, przyjąć można, że liczba certyfikatów zwiększy się o 1/3, tj. wydanych będzie 60 certyfikatów. Projektodawca dopuszcza w projekcie możliwość certyfikacji podejmowanej zarówno przez Prezesa Urzędu, jak i przedsiębiorców i bardzo trudno jest w chwili obecnej przesądzić, który model będzie częściej wykorzystywany. Nie jest możliwe przesądzenie jaka ilość z tej liczby zdecyduje się więc na certyfikację podejmowaną przez przedsiębiorców. Z jednej strony możliwe jest bowiem przyjęcie, że certyfikat wydany przez Prezesa Urzędu będzie wydawał się wizerunkowo silniejszy i bardziej popularny. Z drugiej strony nie jest wykluczone, że przedsiębiorcy mogą obawiać się certyfikacji podejmowanej przez Prezesa Urzędu w związku z ryzykiem wykrycia w toku czynności certyfikacyjnych nieprawidłowości. 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 czynności 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.

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							
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	jw.						
	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 finansowania, 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 będzie się wiązało 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 wspomagającą 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 finansowania, działalności wg kodu PKD oraz nazwy we wskazanych przypadkach. **Zmiana polegająca na nałożeniu obowiązku na przedsiębiorców powołujących inspektorów ochrony danych do 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 (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. Liczba 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 publicznych (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 6023 podmiotów. Rejestr Usług Płatniczych na dzień 11 lipca 2017 r. wynosi 12 936 podmiotów. W przybliżeniu liczba 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 powołujące 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 1100 podmiotów.** Projekt nie będzie miał wpływu na gospodarstwa domowe, gdyż projektowanie rozwiązania dotyczą jedynie podmiotów wskazanych w pkt 4 osr.

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 2016/679 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 ustawy 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 2016/679 oraz projekt ustawy o ochronie danych osobowych znosi ogólny obowiązek dokumentacyjny w zakresie ochrony danych osobowych. Został on zastąpiony zasadą rozliczalności.
– Mając na uwadze ustawowe terminy przewidziane w Kodeksie postępowania administracyjnego, dla załatwienia sprawy w postępowaniu odwoławczym (1 miesiąc), należy przyjąć, iż prowadzenie jednoinstancyjnego postępowania administracyjnego – co oznacza rezygnację z postępowania odwoławczego – spowoduje skrócenie postępowania o co najmniej miesiąc. Mając na uwadze fakt, że postępowania odwoławcze w praktyce mogą trwać dłużej (zgodnie z właściwymi przepisami Kodeksu postępowania administracyjnego) wydaje się, iż jednoinstancyjne postępowanie w sposób istotny skróci czas rozpatrywania spraw, szczególnie w początkowym okresie stosowania rozporządzenia i kształtowania się na tym etapie praktyki orzeczniczej i doktrynalnej.

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 po 20 dniach od publikacji w Dzienniku Urzędowym UE. Rozporządzenie 2016/679 będzie bezpośrednio obowiązujące, skuteczne oraz stosowane od 25 maja 2018 r. i w 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

Warszawa, 08 lutego 2018 r.

Raport

z konsultacji publicznych projektu ustawy o ochronie danych osobowych (UODO)

Projekt ustawy o ochronie danych osobowych (UODO) został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny w dniu 14 września 2017 r. (numer wykazu UC101).

W dniu 14 września 2017 r. Minister Cyfryzacji wystosował zaproszenie do zaopiniowania projektu - było ono wysłane bezpośrednio na adresy e-mail do organizacji społecznych, związków pracodawców i stowarzyszeń branżowych w łącznej liczbie 189 podmiotów.

Równolegle informacja o rozpoczęciu konsultacji społecznych (wraz z projektem ustawy w wersji z dn. 13.09.2017 r.) ukazała się na stronie internetowej Ministerstwa Cyfryzacji www.mc.gov.pl (zakładka konsultacje społeczne) i zaproszenie do udziału w nich było szeroko dystrybuowane w mediach społecznościowych (statystyki dostępne pod linkiem: http://blog.mc.gov.pl/?p=153). Dla potrzeb przyjmowania uwag w domenie mc.gov.pl stworzono dedykowany projektowi adres e-mail: konsultacje.odo@mc.gov.pl.

W toku konsultacji społecznych, trwających do 13 października 2017 r., opinie do ustawy zgłosiło ponad 110 organizacji i obywateli, którzy zgłosili w sumie 641 uwag (tabel z ich zestawieniem jest dostępna na stronie: http://legislacja.rcl.gov.pl/projekt/12302950.

Na zaproszenie aktywnie zareagowały osoby fizyczne, organizacje i firmy (w kolejności alfabetycznej): $(ISC)^2$ Poland Chapter, Amerykańska Izba Handlowa w Polsce, Aspire (kancelarie członkowskie: Raczkowski Paruch oraz Wardyński i wspólnicy), C&C Kancelaria prawna Ciszek sp.k., Clifford Chance, ENSIS Kancelaria Doradztwa Prawnego, Cioczek & Szajdziński Spółka Cywilna, eRecruitment Solutions sp. z o.o, Europejska Federacja Doradców Finansowych Polska – EFFP Polska, Fundacja Bezpieczeństwa Informacji Polska, Fundacja Bezpieczna Cyberprzestrzeń, Fundacja Centrum Analiz dla Rozwoju (Pilch Piotrowski i Partnerzy Adwokacka Spółka Partnerska), Fundacja Dajemy Dzieciom Siłę, Fundacja ePaństwo, Fundacja Panoptykon, Fundacja Rozwoju Rynku Finansowego, Grupa Doradcza Sienna Sp. z o.o, IAB

Polska (Związek Pracodawców Branży Internetowej), INFARMA Związek Pracodawców Innowacyjnych Firm Farmaceutycznych, Instytut Łączności, Instytut Maszyn Matematycznych, ISACA, Izba Domów Maklerskich, Izba Gospodarcza Hotelarstwa Polskiego, Izba Gospodarcza Towarzystw Emerytalnych, Izba Gospodarki Elektronicznej, Izba Wydawców Prasy, Izba Zarządzających Funduszami i Aktywami (IZFiA), Kancelaria Prawna HTP Puniewska Waszczyńska Spółka Komandytowa z siedzibą we Wrocławiu, Katedra Prawa Cywilnego i Prawa Prywatnego Międzynarodowego WPiA UKSW, Komitet Sterujący Polskiej Federacji Szpitali w składzie: Fundacja Telemedycyna, Porozumienie Zielonogórskie, Medicover i Związek Pracodawców Technologii Cyfrowych, Konfederacja Lewiatan, Konfederacja Przedsiębiorstw Finansowych w Polsce, Konferencja Rektorów Akademickich Szkół Polskich, KONTOMATIK - Kontomierz.pl sp. z o.o., Krajowa Izba Gospodarcza, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, Krajowa Izba Rozliczeniowa, Krajowa Rada Komornicza, Krajowa Rada Kuratorów, Krajowa Spółdzielcza Kasa Oszczędnościowo – Kredytowa, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Largo Law, Microsoft Sp. z o.o., MIKROBIT Sp. z o.o., Naczelna Izba Lekarska, Naczelna Izba Pielęgniarek i Położnych, NASK, Ogólnopolskie Porozumienie Związków Zawodowych, Persona, PGNiG, Polska Izba Informatyki i Telekomunikacji [Pii T], Polska Izba Ochrony, Polska Izba Ubezpieczeń (PIU), Polska Organizacja Handlu i Dystrybucji (POHiD), Polska Organizacja Niebankowych Instytucji Płatności Związek Pracodawców, Polska Organizacja Przemysłu i Handlu Naftowego POPiHN, Polska Unia Szpitali Klinicznych, Polski Związek Instytucji Pożyczkowych (dawniej Związek Firm Pożyczkowych), Polski Związek Pracodawców Przemysłu Farmaceutycznego, Polski Związek Instytucji Pożyczkowych, Polski Związek Łowiecki, Polskie Biuro Ubezpieczycieli Komunikacyjnych, Polskie Forum HR, Polskie Stowarzyszenie Marketingu SMB, Polskie Towarzystwo Informatyczne PIT, Porozumienie Pracodawców Ochrony Zdrowia, Porozumienie Zielonogórskie, Porozumieniu Pracodawców Ochrony Zdrowia, Pracodawcy RP, Prezydium KK NSZZ „Solidarność”, SENDERO TAX & LEGAL, Stowarzyszenia Dziennikarzy i Wydawców REPROPOL, Stowarzyszenie Administratorów Bezpieczeństwa Informacji (SABI), Stowarzyszenie Autorów ZAiKS, Stowarzyszenie Dziennikarzy Rzeczypospolitej Polskiej Zarząd Główny, Stowarzyszenie Inspektorów Ochrony Danych Osobowych, Stowarzyszenie ISSA Polska, Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej, Śląska Izba Lekarska, TI-KONSULTING, Ubezpieczeniowy Fundusz Gwarancyjny, Urbanek i Wspólnicy, Związek Pracodawców POLSKA MIEDŹ, Związek Banków Polskich, Związek Pracodawców Business Center Club, Związek Pracodawców

Przemysłu Farmaceutycznego oraz Związek Pracodawców Technologii Cyfrowych Lewiatan.

Projekt spotkał się z ogólnym dobrym odbiorem opiniujących, o czym świadczą przykłady wypowiedzi, przytoczone poniżej, zaś liczba zgłoszonych uwag świadczy o wspólnej trosce o jakość ostatecznego kształtu ustawy.

„Na wstępie IAB Polska pragnie podkreślić, iż z aprobatą przyjmuje uchylenie przepisów rozdziału IV ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. IAB Polska podziela pogląd Ministra Cyfryzacji, że RODO swoim zakresem podmiotowym i przedmiotowym obejmuje przetwarzanie danych osobowych w związku ze świadczeniem usług drogą elektroniczną (regulowanych treścią uśude).

Należy także zwrócić uwagę na kompromis, który został osiągnięty w sprawie zgody na przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego (zgoda na cookies) na gruncie Prawa Telekomunikacyjnego.

*IAB Polska z zadowoleniem przyjmuje zaproponowanie wyłączenia w art. 2 ust. 1 projektu (należy przypomnieć, że podmioty prowadzące serwisy internetowe także mogą zostać uznane za prasę).” /**IAB Polska/***

„Pozytywnie należy co do zasady ocenić rozwiązanie przyznające Prezesowi UODO uprawnienie do wydawania postanowień zabezpieczających zobowiązujących wskazany w nich podmiot do ograniczenia przechowywania danych osobowych, o których mowa w art. 53 projektu.

*Pozytywnie należy ocenić propozycje uregulowania statusu prawnego adwokatów jako podmiotów przetwarzających dane osobowe.” /**Naczelna Rada Adwokacka/***

*„Konfederacja Lewiatan („Konfederacja”) wyraża zadowolenie, iż część istotnych uwag, formułowanych przez Konfederację na wcześniejszych etapach nieformalnych, szeroko zakrojonych konsultacji, zostało przez Projektodawcę uwzględnionych i znajduje swój wyraz w brzmieniu przedłożonych do konsultacji publicznych projektów ustaw.” /**Konfederacja Lewiatan/***

„Ministerstwo Cyfryzacji dobrze poradziło sobie z zadaniem wdrożenia RODO. Jednak obok pochwał musimy zgłosić kilka poważnych zastrzeżeń.

Pozytywnie oceniamy przyjęcie rozwiązania, zgodnie z którym Prezes Urzędu będzie organem nadzorczym w rozumieniu dyrektywy policyjnej. Naszym zdaniem powierzenie realizacji zadań nadzorczych wynikających z RODO

i dyrektywy policyjnej jednemu organowi zwiększy jego efektywność i spójność podejmowanych działań.

Pozytywnie oceniamy propozycję powołania Rady do spraw ochrony danych osobowych jako organu doradczego Prezesa.

Popieramy konstrukcję, zgodnie z którą organ nadzorczy będzie mógł nakładać na podmioty publiczne kary finansowe. Takie rozwiązanie może wpłynąć w pozytywny sposób na faktyczny poziom ochrony praw obywateli. Z drugiej strony zrozumiała jest decyzja o obniżeniu maksymalnej wysokości kary finansowej w przypadku organów publicznych w porównaniu do działalności podmiotów komercyjnych. Popieramy także wymóg udostępniania na stronach internetowych decyzji PUODO podejmowanych wobec organów publicznych oraz publikowania informacji o działaniach, które mają na celu wykonanie ww. decyzji." **/Fundacja Panoptykon /**

Wstępne podsumowanie konsultacji społecznych, zakończonych w dniu 13 października 2017 r., odbyło się na śniadaniu prasowym, zorganizowanym przez Ministra Cyfryzacji w dniu 24 października 2017 r.

W toku dalszych prac Projektodawca poddał wnikliwej ocenie wszystkie zgłoszone uwagi, odnosząc się w tabeli, opublikowanej na stronie RCL.

Stanowisko Ministra Cyfryzacji wobec uwag zgłoszonych w konsultacjach projektu UODO zostało szczegółowo omówione na Konferencji, która odbyła się w Sali Kolumnowej Sejmu Rzeczypospolitej Polskiej w dniu 15 stycznia 2018 r.

Zaproszenie do udziału w niej było opublikowane na stronie internetowej www.mc.gov.pl i dystrybuowane w mediach społecznościowych. Wstępna zapowiedź planu organizacji Konferencji była opublikowana na blogu Ministra Cyfryzacji w październiku 2017 r. (http://blog.mc.gov.pl/?p=80). Na ten anons zareagowało potwierdzeniem chęci osobistego udziału w wydarzeniu blisko 250 osób.

Po ogłoszeniu terminu i miejsca Konferencji udział w niej potwierdziło ponad 400 osób. Ostatecznie w wydarzeniu uczestniczyło osobiście około 300 osób. Zainteresowani mogli także śledzić przebieg debaty w relacji na żywo, której nagranie nadal dostępne jest na stronie: http://www.sejm.gov.pl/Sejm8.nsf/transmisje_arch.xsp?unid=C14F7FC92D434C42C125820F0031601D

Na konferencji omówiono szczegółowo tematy, w odniesieniu do których wpłynęło szczególnie dużo uwag (ich listę zawiera załączona tabela).

Ponadto od połowy września 2017 r. Dyrektor Departamentu Zarządzania Danymi, uczestniczył w ponad 40 konferencjach, organizowanych w Warszawie i innych miastach przez organizacje społeczne i/lub stowarzyszenia branżowe, na których obok prezentacji najistotniejszych założeń Rozporządzenia UE 2016/670 zbierał opinie i komentarze, odnoszące się do wątpliwości czy zastrzeżeń dotyczących projektowanych przepisów krajowych. Wszystkie były poddawane szczegółowej analizie zespołu pracującego nad ostateczną treścią projektu ustawy.

Do wszystkich głosów i zgłoszonych uwag oraz zastrzeżeń projektodawca ustosunkował się z najwyższą starannością, mając na względzie zarówno troskę o zgodność projektowanych przepisów krajowych z rozporządzeniem UE, jak również głosy organizacji.

Lista zagadnień omówionych podczas konferencji 15 stycznia 2018 r.

Dysproporcje w wysokości kar/ Dlaczego niższe kary dla administracji
Powołanie Prezesa Urzędu (tryb powołania)
IOD - powołanie, niezależność, zadania, kiedy obowiązkowy
Działalność dziennikarska, literacka itd.
Konsultacje społeczne – dobre praktyki
Wiek dziecka: granica, problemy, weryfikacja rodzica
Ewidencja zawiadomień o wyznaczeniu IOD = system teleinformatyczny
Podpis elektroniczny
Podmiot dokonujący certyfikacji
Publikacja kryteriów certyfikacji w BIP
Wniosek o certyfikację i jego rozpatrzenie
Przeprowadzenie przez Prezesa Urzędu czynności sprawdzających u administratora lub podmiotu przetwarzającego w celu oceny spełniania przez ten podmiot kryteriów certyfikacji
Opłata za czynności związane z postępowaniem o udzielenie certyfikacji
Monitorowanie przestrzegania zatwierdzonego kodeksu postępowania oraz akredytacja
PUODO, kryteria, wymagania itd.
Powołanie, odwołanie PUODO
Zastępcy PUODO
PUODO a inna działalność
Rada PUODO
Wystąpienia PUODO - czy wiążące
Wykaz operacji do oceny skutków
Kodeksy postępowania
Rekomendacje PUODO
Jednoinstancyjność postępowania

Udział i uprawnienia organizacji społecznej w postępowaniu dotyczącym naruszenia praw osoby
Zawiadamianie przez Prezesa Urzędu stron o niezałatwianiu sprawy w terminie
Dostęp Prezesa Urzędu do informacji, w tym informacji zawierających tajemnicę przedsiębiorstwa oraz ustawowo chronionych oraz ograniczenie prawa do wglądu
Kara grzywny za niestawienie się bez uzasadnionej przyczyny jako świadek lub biegły albo bezzasadną odmowę złożenia zeznania, brak przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej
Postanowienie dotyczące ograniczenia przetwarzania
Decyzja o umorzeniu postępowania
Rygor natychmiastowej wykonalności decyzji Prezesa UODO oraz tryb zaskarżenia decyzji
Niezbędne środki w trakcie kontroli
Postępowanie kontrolne (nieobecność kontrolowanego, uprawnienia przyznane kontrolującym, korzystanie z pomocy funkcjonariuszy, nagrywanie kontroli, odmowa udzielenia informacji)
Protokół pokontrolny
Odpowiedzialność osób fizycznych
Roszczenia z tytułu naruszenia
Termin płatności kary
Fundusz Ochrony Danych
Bezpodstawne przetwarzanie danych
Kompetencje PUODO zarówno do dokonywania certyfikacji jak i prowadzenia postępowań w sprawie naruszenia przepisów

TYTUŁ PROJEKTU:	Ustawa o ochronie danych osobowych				
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO / WDRAŻANYCH AKTÓW PRAWNYCH [1]:	1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27kwietnia 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)				

PRZEPISY UNII EUROPEJSKIEJ [2]					
Jedn. red.	**Treść przepisu UE [3]**	**Koniecz-ność wdrożenia** T / N	**Jedn. red. (*)**	**Treść przepisu/ów projektu (*)**	**Uzasadnienie uwzględnienia w projekcie przepisów wykraczających poza minimalne wymogi prawa UE (**)**
1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27kwietnia 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)					
Uwaga: Rozporządzenie będzie stosowane bezpośrednio i jego przepisy nie podlegają transpozycji do prawa krajowego. W rozporządzeniu znajdują się dyspozycje dla państw członkowskich, które wymagają dostosowania przepisów krajowych w celu zapewnienia efektywnego stosowania regulacji wspólnotowych.					
Rozdział I					
Przepisy ogólne					
Art. 1	**Przedmiot i cele** 1. W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych. 2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. 3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.	**N**			
Art. 2	**Materialny zakres stosowania** 1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. 2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych: a) w ramach działalności nieobjętej zakresem prawa Unii; b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE; c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze; d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia	**T**	**Art. 1 ust. 1**	**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”.	

	postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. 3. Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98. 4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy.				
Art. 3	**Terytorialny zakres stosowania** 1. Niniejsze rozporządzenie ma zastosowanie 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. 2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających 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. 3. Niniejsze rozporządzenie ma zastosowanie 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.	**T**	**Art. 1 ust. 1**	**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”.	
Art. 4	**Definicje** Na użytek niniejszego rozporządzenia: 1) „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; 2)„przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany	**N**			

	lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie; 3) „ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania; 4) „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się; 5) „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 6) „zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie; 7) „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania; 8) „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora; 9) „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane 4.5.2016 L 119/33 Dziennik Urzędowy Unii Europejskiej PL osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania; 10) „strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot				

	przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe; 11) „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych; 12) „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych; 13) „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej; 14) „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne; 15) „dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia; 16) „główna jednostka organizacyjna” oznacza: a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje; b) jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia; 17) „przedstawiciel” oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;				

	18) „przedsiębiorca” oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą; 19) „grupa przedsiębiorstw” oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane; 20) „wiążące reguły korporacyjne” oznaczają polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą; 21) „organ nadzorczy” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51; 22) „organ nadzorczy, którego sprawa dotyczy” oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ: a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego; b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub c) wniesiono do niego skargę; 23) „transgraniczne przetwarzanie” oznacza: a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim; 24) „mający znaczenie dla sprawy i uzasadniony sprzeciw” oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii; 25) „usługa społeczeństwa informacyjnego” oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1); 26) „organizacja międzynarodowa” oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.				

Rozdział II **Zasady**					
Art. 5	**Zasady dotyczące przetwarzania danych osobowych** 1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”); b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”); e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”). 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).	**N**			

Art. 6	**Zgodność przetwarzania z prawem** 1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. 2. Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów niniejszego rozporządzenia w odniesieniu do przetwarzania służącego wypełnieniu warunków określonych w ust. 1 lit. c) i e); w tym celu mogą dokładniej określić szczegółowe wymogi przetwarzania i inne środki w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, także w innych szczególnych sytuacjach związanych z przetwarzaniem przewidzianych w rozdziale IX. 3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.	**N**			

	4. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi: a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania; b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem; c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10; d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.				
Art. 7	**Warunki wyrażenia zgody** 1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. 2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca. 3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. 4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.	**N**			
Art. 8	**Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego** 1. Jeżeli zastosowanie ma art. 6 ust. 1 lit. a), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest	**N**			

	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. 2. W takich przypadkach administrator, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała. 3. Ust. 1 nie wpływa na ogólne przepisy prawa umów państw członkowskich, takie jak przepisy o ważności, zawieraniu lub skutkach umowy wobec dziecka**.**				

Art. 9	**Przetwarzanie szczególnych kategorii danych osobowych** 1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. 2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków: a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1; b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą; c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą; e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą; f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy; g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą; h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3; i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów	**N**			

	leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową; j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. 3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe. 4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.				
Art. 10	**Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa** Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych**.**	**N**			
Art. 11.	**Przetwarzanie niewymagające identyfikacji** 1. Jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia. 2. Jeżeli w przypadkach, o których mowa w ust. 1 niniejszego artykułu, administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. W takich przypadkach zastosowania nie mają art. 15–20, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować.	**N**			

ROZDZIAŁ III **Prawa osoby, której dane dotyczą**					
SEKCJA 1 **Przejrzystość oraz tryb korzystania z praw**					
Art. 12	**Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą** 1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. 2. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22. W przypadkach, o których mowa w art. 11 ust. 2, administrator nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 15–22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą. 3. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. 4. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem. 5. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może: a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo b) odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze. 6. Bez uszczerbku dla art. 11, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21,	**N**			

	może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. 7. Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego. 8. Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych.				
SEKCJA 2 **Informacje i dostęp do danych osobowych**					
Art. 13	**Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą** 1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje: a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych; c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania; d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych. 2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania: a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu; b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec	**N**			

	przetwarzania, a także o prawie do przenoszenia danych; c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; d) informacje o prawie wniesienia skargi do organu nadzorczego; e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych; f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. 3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2. 4. Ust. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.				
Art. 14	**Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą** 1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje: a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych; c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania; d) kategorie odnośnych danych osobowych; e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych. 2. Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą: a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;	**N**			

	b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; e) informacje o prawie wniesienia skargi do organu nadzorczego; f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych; g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. 3. Informacje, o których mowa w ust. 1 i 2, administrator podaje: a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych; b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu. 4. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2. 5. Ust. 1– 4 nie mają zastosowania, gdy – i w zakresie, w jakim: a) osoba, której dane dotyczą, dysponuje już tymi informacjami; b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie; c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania				

	tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.				
Art. 15	**Prawo dostępu przysługujące osobie, której dane dotyczą** 1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji: a) cele przetwarzania; b) kategorie odnośnych danych osobowych; c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu; e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania; f) informacje o prawie wniesienia skargi do organu nadzorczego; g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle; h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. 2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem. 3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. 4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.	**N**			
SEKCJA 3 **Sprostowanie i usuwanie danych**					
Art. 16	**Prawo do sprostowania danych** Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z	**N**			

	uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.				
Art. 17	**Prawo do usunięcia danych („prawo do bycia zapomnianym")** 1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności: a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane; b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania; c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania; d) dane osobowe były przetwarzane niezgodnie z prawem; e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator; f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1. 2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. 3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne: a) do korzystania z prawa do wolności wypowiedzi i informacji; b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3; d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub e) do ustalenia, dochodzenia lub obrony roszczeń.	**N**			

Art. 18	**Prawo do ograniczenia przetwarzania** 1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach: a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych; b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń; d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą. 2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego. 3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.	**N**			
Art. 19	**Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania** Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.	**N**			
Art. 20	**Prawo do przenoszenia danych** 1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli: a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz b) przetwarzanie odbywa się w sposób zautomatyzowany. 2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez	**N**			

	administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. 3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. 4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.				
SEKCJA 4 **Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach**					
Art. 21	**Prawo do sprzeciwu** 1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. 2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. 3. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów. 4. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji. 5. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne. 6. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie	**N**			

	publicznym				
Art. 22	**Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie** 1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. 2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja: a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą. 3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. 4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.	**N**			
SEKCJA 5 **Ograniczenia**					
Art. 23	**Ograniczenia** 1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym: a) bezpieczeństwu narodowemu; b) obronie; c) bezpieczeństwu publicznemu; d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim	**N**	**Art. 3** **Art. 4** **Art. 5**	**Art. 3.** 1. Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679, jeżeli zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 13 ust. 3 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji: 1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego, lub 2) naruszy ochronę informacji niejawnych.	

	zagrożeniom; e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu; f) ochronie niezależności sądów i postępowania sądowego; g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu; h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) – e) oraz g); i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób; j) egzekucji roszczeń cywilnoprawnych. 2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o: a) celach przetwarzania lub kategorii przetwarzania; b) kategoriach danych osobowych; c) zakresie wprowadzonych ograniczeń; d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu; e) określeniu administratora lub kategorii administratorów; f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania; g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz h) prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.			2. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 3. Administrator jest obowiązany bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca, poinformować osobę, której dane dotyczą, na jej wniosek, o podstawie nieprzekazania informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679. **Art. 4**. 1. W zakresie nieuregulowanym w art. 14 ust. 5 rozporządzenia 2016/679, administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji: 1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego, lub 2) naruszy ochronę informacji niejawnych. 2. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 3. Administrator jest obowiązany bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca, poinformować osobę, której dane dotyczą, na jej wniosek, o podstawie nieprzekazania informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679. **Art. 5.** 1. Przepisów, o których mowa w art. 15 ust. 1-3 rozporządzenia 2016/679, nie stosuje się w przypadku gdy osoba, której dane dotyczą, nie jest informowana na podstawie art. 4 ust. 1. 2. W przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 rozporządzenia 2016/679, wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, administrator wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Przepis art. 64 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149) stosuje się odpowiednio.	

				3. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 4. Administrator jest obowiązany bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca, poinformować osobę, której dane dotyczą, na jej wniosek, o podstawie nieprzekazania informacji, o których mowa w art. 15 ust. 1 i 3 rozporządzenia 2016/679.	
ROZDZIAŁ IV **Administrator i podmiot przetwarzający**					
SEKCJA 1 **Obowiązki ogólne**					
Art. 24	**Obowiązki administratora** 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych. 3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.	**N**			
Art. 25	**Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych** 1. 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 wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. 2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla	**N**			

	osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.				
Art. 26	**Współadministratorzy** 1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień Współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. 2. Uzgodnienia, o których mowa w ust. 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą. 3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.	**N**			
Art. 27	**Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii** 1. Jeżeli zastosowanie ma art. 3 ust. 2, administrator lub podmiot przetwarzający na piśmie wyznacza swojego przedstawiciela w Unii. 2. Obowiązek ustanowiony w ust. 1 niniejszego artykułu nie ma zastosowania w przypadku: a) przetwarzania, które ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, ani przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych; lub b) organu lub podmiotu publicznego. 3. Przedstawiciel musi mieć siedzibę w państwie członkowskim, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przetwarzane w	**N**			

	związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane. 4. Przedstawiciel zostaje upoważniony przez administratora lub podmiot przetwarzający, by do celów zapewnienia przestrzegania niniejszego rozporządzenia mogły się do niego zwracać – oprócz lub zamiast do administratora lub podmiotu przetwarzającego – w szczególności organy nadzorcze i osoby, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem. 5. Wyznaczenie przedstawiciela przez administratora lub podmiot przetwarzający pozostaje bez uszczerbku dla postępowań, które mogą zostać wszczęte przeciwko samemu administratorowi lub podmiotowi przetwarzającemu.				
Art. 28	**Podmiot przetwarzający** 1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. 2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. 3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający: a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny; b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy; c) podejmuje wszelkie środki wymagane na mocy art. 32;	**N** **N** **N**			

	d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4; e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III; f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36; g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych; h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.				
	4. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.	**N**			
	5. Wystarczające gwarancje, o których mowa w ust. 1 i 4 niniejszego artykułu, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.	**N**			
	6. Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 3 i 4 niniejszego artykułu, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 7 i 8 niniejszego artykułu, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43.	**N**			
	7. Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.	**N**			

	8. Organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z mechanizmem spójności, o którym mowa w art. 63. 9. Umowa lub inny akt prawny, o których mowa w art. 3 i 4, mają formę pisemną, w tym formę elektroniczną. 10. Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.	**T** **N** **N**	**Art. 54 ust. 1 pkt 1**	**Art. 54**. 1. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej: 1) standardowe klauzule umowne, o których mowa w art. 28 ust. 8 rozporządzenia 2016/679;	
Art. 29	**Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego** Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.	**N**			
Art. 30	**Rejestrowanie czynności przetwarzania** 1. Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje: a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych; b) cele przetwarzania; c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych; e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń; f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. 2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:	**N**			

	a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych; b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów; c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń; d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. 3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną. 4. Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego. 5. Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.				
Art. 31	**Współpraca z organem nadzorczym** Administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.	**N**			
SEKCJA 2 **Bezpieczeństwo danych osobowych**					
Art. 32	**Bezpieczeństwo przetwarzania** 1. 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, w tym między innymi w stosownym przypadku: a) pseudonimizację i szyfrowanie danych osobowych; b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.	**T**	**Art. 54**	**Art. 54.** 1. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej: 1) standardowe klauzule umowne, o których mowa w art. 28 ust. 8 rozporządzenia 2016/679; 2) zatwierdzone kodeksy postępowania, o których mowa w art. 40 rozporządzenia 2016/679, a także zmiany tych kodeksów; 3) przyjęte standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit d rozporządzenia 2016/679; 4) rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. 2. Rekomendacje, o których mowa w ust. 1 pkt 4, sporządzane są z uwzględnieniem specyfiki danego	

	2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42. 4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.			rodzaju działalności i podlegają okresowej aktualizacji. 3. Projekt rekomendacji, o których mowa w ust. 1 pkt 4, Prezes Urzędu konsultuje z zainteresowanymi podmiotami, których zakresu działania dotyczy dany projekt.	
Art. 33	**Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu** 1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. 2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. 3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej: a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych; d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków. 4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki. 5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte	**T** **N** **N** **N** **N**	**Art. 56**	**Art. 56**. Prezes Urzędu może prowadzić system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679.	

	działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.				
Art. 34	**Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych** 1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. 2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d). 3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach: a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1; c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. 4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.	**N**			
SEKCJA 3 **Ocena skutków dla ochrony danych i uprzednie konsultacje**					
Art. 35	**Ocena skutków dla ochrony danych** 1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. 2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.	**N** **N**			

	3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku: a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.	**N**			
	4. Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68. 5. Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.	**T**	**Art. 55**	**Art. 55**. 1. Prezes Urzędu: 1) ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679; 2) może ogłosić w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych niewymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 5 rozporządzenia 2016/679. 2. Komunikat, o którym mowa w ust. 1, ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.	
	6. Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.	**N**			
	7. Ocena zawiera co najmniej: a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób,	**N**			

	których sprawa dotyczy. 8. Oceniając – w szczególności do celów oceny skutków dla ochrony danych – skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40. 9. W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania. 10. Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych. 11. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.	**N** **N** **N** **N**			
Art. 36	**Uprzednie konsultacje** 1. Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. 2. Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie niniejszego rozporządzenia – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela administratorowi, a gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemnego zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58. Okres ten można przedłużyć o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje administratora, a gdy ma to zastosowanie także podmiot przetwarzający, o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji. 3. Konsultując się z organem nadzorczym zgodnie z ust. 1, administrator przedstawia mu: a) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w	**T**	**Art. 58**	**Art. 58.** 1. Administrator danych lub podmiot przetwarzający może wystąpić do Prezesa Urzędu z wnioskiem o przeprowadzenie uprzednich konsultacji, o którym mowa w art. 36 rozporządzenia 2016/679. 2. Do wniosku stosuje się odpowiednio art. 63 ustawy z dnia 14 czerwca 1960 r - Kodeks postępowania administracyjnego. 3. Jeżeli wniosek nie spełnia wymogów, określonych w art. 36 ust. 3 rozporządzenia 2016/679 oraz w art. 63 ustawy z dnia 14 czerwca 1960 r - Kodeks postępowania administracyjnego, Prezes Urzędu informuje o nieudzieleniu konsultacji wskazując przyczyny jej nieudzielenia.	

	przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw; b) cele i sposoby zamierzonego przetwarzania; c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem; d) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych; e) ocenę skutków dla ochrony danych, o której mowa w art. 35; oraz f) wszelkie inne informacje, których żąda organ nadzorczy. 4. Państwa członkowskie konsultują się z organem nadzorczym, przygotowując projekt aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania. 5. Niezależnie od ust. 1 prawo państwa członkowskiego może wymagać, by administratorzy konsultowali się z organem nadzorczym i uzyskiwali jego uprzednią zgodę na przetwarzanie danych osobowych przez administratora do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym.				
Sekcja 4 **Inspektor ochrony danych**					
Art. 37	**Wyznaczenie inspektora ochrony danych** 1. 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;	**T**	**Art. 9** **Art. 10**	**Art. 9.** Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się: 1) jednostki sektora finansów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych; 2) instytuty badawcze, o których mowa w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2017 r. poz. 1158, 1452 i 2201); 3) Narodowy Bank Polski. **Art. 10**. 1. Podmiot, który wyznaczył inspektora zawiadamia Prezesa Urzędu o jego wyznaczeniu, w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora. 2. Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, o którym mowa w ust. 1. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej. 3. W zawiadomieniu obok danych, o których mowa w ust. 1, wskazuje się:	

				1) imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna; 2) firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą; albo 3) pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 albo 2; 4) numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu. 4. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu, o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania. 5. W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorstw, każdy z tych podmiotów dokonuje zawiadomienia, o którym mowa w ust. 1 i 4. 6. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.	
	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	**N**			
	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.	**N**			
	2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.	**N**			
	3. 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.	**N**			
	4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot	**N**			

	przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające. 5. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39. 6. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. 7. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.	**N** **N** **T**	**Art.11** **Art. 12**	**Art. 11.** Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności. A**rt. 12.** Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.	
Art. 38	**Status inspektora ochrony danych** 1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. 2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. 3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega	**N**			

	najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. 4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. 5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. 6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.				
Art. 39	**Zadania inspektora ochrony danych** 1. Inspektor ochrony danych ma następujące zadania: a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie; b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty; c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35; d) współpraca z organem nadzorczym; e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach. 2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.	**N**			
SEKCJA 5 **Kodeksy postępowania i certyfikacja**					
Art. 40	**Kodeksy postępowania** 1. 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 małych i średnich przedsiębiorstw. 2. Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy	**N**			

	postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie niniejszego rozporządzenia, między innymi w odniesieniu do: a) rzetelnego i przejrzystego przetwarzania; b) prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach; c) zbierania danych osobowych; d) pseudonimizacji danych osobowych; e) informowania opinii publicznej i osób, których dane dotyczą; f) wykonywania przez osoby, których dane dotyczą, przysługujących im praw; g) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem; h) środków i procedur, o których mowa w art. 24 i 25, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32; i) zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą; j) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych; lub k) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79. 3. Poza administratorami lub podmiotami przetwarzającymi, którzy podlegają niniejszemu rozporządzeniu, kodeksów postępowania zatwierdzonych na mocy ust. 5 niniejszego artykułu i powszechnie obowiązujących zgodnie z ust. 9 niniejszego artykułu, mogą przestrzegać także administratorzy lub podmioty przetwarzające, którzy zgodnie z art. 3 nie podlegają niniejszemu rozporządzeniu, w celu zapewnienia odpowiednich zabezpieczeń w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 46 ust. 2 lit. e). Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązanie – w drodze umowy lub poprzez inne prawnie wiążące instrumenty – do stosowania tych odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. 4. Kodeks postępowania, o którym mowa w ust. 2 niniejszego artykułu, przewiduje mechanizmy pozwalające podmiotowi, o którym mowa w art. 41 ust. 1, prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu przez administratorów lub podmioty przetwarzające, którzy podjęli się jego stosowania, bez uszczerbku dla zadań i uprawnień organów nadzorczych właściwych na mocy art. 55 lub 56. 5. Zrzeszenia i inne podmioty, o których mowa w ust. 2 niniejszego artykułu, chcące opracować kodeks postępowania lub zmienić lub rozszerzyć zakres kodeksu już obowiązującego przedkładają projekt kodeksu, zmiany lub rozszerzenia organowi nadzorczemu właściwemu na mocy art. 55. Organ nadzorczy wydaje opinię o zgodności projektu kodeksu, zmiany lub rozszerzenia z niniejszym rozporządzeniem i zatwierdza taki projekt kodeksu, zmiany lub rozszerzenia, jeżeli uzna, że stanowią one odpowiednie zabezpieczenia.	**N** **N** **T**	**Art. 27**	**Art. 27**. 1. Kodeks postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, zwany dalej „kodeksem postępowania" jest opracowywany, opiniowany i zatwierdzany na zasadach określonych w tym rozporządzeniu. 2. Kodeks postępowania przed przekazaniem do zatwierdzeniem Prezesowi Urzędu podlega konsultacjom z zainteresowanymi podmiotami. 3. Informację o przeprowadzonych konsultacjach oraz ich wyniku przekazuje się Prezesowi Urzędu wraz z	

				kodeksem postępowania. 4. W przypadku uznania przez Prezesa Urzędu zakresu konsultacji za niewystarczający, wyzywa on podmiot do przeprowadzenia ponownych konsultacji, wskazując ich zakres. 5. Stroną postępowania w sprawie zatwierdzenia kodeksu postępowania jest wyłącznie wnioskodawca występujący o zatwierdzenie tego kodeksu. Przepisu art. 31 ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego, nie stosuje się. 6. Do zmiany zatwierdzonego kodeksu postępowania lub jego rozszerzenia stosuje się ust. 1-5.	
	6. W przypadku zatwierdzenia zgodnie z ust. 5 projektu kodeksu, zmiany lub rozszerzenia, organ nadzorczy rejestruje i publikuje ten kodeks, o ile nie dotyczy on czynności przetwarzania prowadzonych w kilku państwach członkowskich.	**T**	**Art. 54 ust. 1 pkt 2**	**Art. 54**. 1. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej: 2) zatwierdzone kodeksy postępowania, o których mowa w art. 40 rozporządzenia 2016/679, a także zmiany tych kodeksów;	
	7. Jeżeli projekt kodeksu postępowania dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, organ nadzorczy właściwy na mocy art. 55 przed zatwierdzeniem projektu kodeksu, zmiany lub rozszerzenia przedkłada go zgodnie z procedurą, o której mowa w art. 63, Europejskiej Radzie Ochrony Danych, która wydaje opinię o zgodności projektu kodeksu, zmiany lub rozszerzenia z niniejszym rozporządzeniem lub w sytuacji określonej w ust. 3 niniejszego artykułu opinię o tym, czy stanowią one odpowiednie zabezpieczenia.	**N**			
	8. Jeżeli opinia, o której mowa w ust. 7, potwierdza, że projekt kodeksu, zmiany lub rozszerzenia jest zgodny z niniejszym rozporządzeniem lub w sytuacji określonej w ust. 3 stanowią odpowiednie zabezpieczenia, Europejska Rada Ochrony Danych przedkłada tę opinię Komisji.	**N**			
	9. Komisja może, w drodze aktów wykonawczych, stwierdzić, że zatwierdzony kodeks postępowania, zmiana lub rozszerzenie przedłożone jej na mocy ust. 8 niniejszego artykułu są powszechnie obowiązujące w Unii. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.	**N**			
	10. Komisja zapewnia odpowiednie upowszechnianie zatwierdzonych kodeksów, których powszechne obowiązywanie stwierdziła zgodnie z ust. 9.	**N**			
	11. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie zatwierdzone kodeksy podstępowania, zmiany i rozszerzenia i udostępnia je opinii	**N**			

	publicznej za pomocą odpowiednich środków.				
Art. 41	**Monitorowanie zatwierdzonych kodeksów postepowania** 1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 monitorowaniem przestrzegania kodeksu postępowania na mocy art. 40 może się zajmować podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez właściwy organ nadzorczy. 2. Podmiot, o którym mowa w ust. 1, może zostać akredytowany w celu monitorowania przestrzegania kodeksu postępowania, jeżeli: a) w sposób satysfakcjonujący wykazał on właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu; b) dysponuje procedurami, które pozwalają mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania; c) dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwalają zapewnić przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz d) w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.	**T**	**Art. 28** **Art. 29**	**Art. 28**. Przestrzeganie zatwierdzonego kodeksu postępowania, monitoruje podmiot akredytowany przez Prezesa Urzędu na zasadach określonych w art. 41 rozporządzenia 2016/679. **Art. 29**. 1. Akredytacja podmiotu, o którym mowa w art. 28, jest udzielana na wniosek, który zawiera co najmniej: 1) nazwę podmiotu ubiegającego się o akredytację oraz adres jego siedziby; 2) informacje potwierdzające spełnianie kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679. 2. Do wniosku dołącza się dokumenty potwierdzające spełnianie kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, albo ich kopie. 3. Wniosek składa się pisemnie w postaci papierowej opatrzonej własnoręcznym podpisem albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.	
	3. Właściwy organ nadzorczy przedkłada proponowane kryteria akredytacji podmiotu, o którym mowa w ust. 1 niniejszego artykułu, Europejskiej Radzie Ochrony Danych zgodnie z mechanizmem spójności, o którym mowa w art. 63.	**N**			
	4. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego oraz przepisów rozdziału VIII podmiot, o którym mowa w ust. 1 niniejszego artykułu – z zastrzeżeniem odpowiednich zabezpieczeń – podejmuje odpowiednie działania w przypadku naruszenia kodeksu przez administratora lub podmiot przetwarzający, w tym zawiesza lub wyklucza administratora lub podmiot przetwarzający spośród stosujących kodeks. O działaniach tych i powodach ich podjęcia informuje on właściwy organ nadzorczy.	**N**			
	5. Właściwy organ nadzorczy cofa akredytację podmiotu, o którym mowa w ust. 1, jeżeli podmiot ten nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania przez niego podejmowane nie są zgodne z niniejszym rozporządzeniem.	**T**	**Art. 32**	**Art. 32**. W okresie na jaki udzielona została akredytacja podmiot akredytowany jest obowiązany spełniać kryteria, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, obowiązujące na dzień wydania certyfikatu akredytacyjnego. 2. Prezes Urzędu cofa w drodze decyzji akredytację w przypadku stwierdzenia, że podmiot akredytowany: 1) nie spełnia lub przestał spełniać kryteria akredytacji, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679; 2) podejmuje działania niezgodne z przepisami rozporządzenia 2016/679.	

	6. Niniejszy artykuł nie ma zastosowania do przetwarzania prowadzonego przez organy i podmioty publiczne.	**N**			
Art. 42	**Certyfikacja** 1. 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 niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.	**N**			
	2. Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych zatwierdzone na mocy ust. 5 niniejszego artykułu, które mają zastosowanie do administratorów lub podmiotów przetwarzających podlegających niniejszemu rozporządzeniu, mogą być ustanowione do wykazania odpowiednich zabezpieczeń przez administratorów lub podmioty przetwarzające, którzy zgodnie z art. 3 nie podlegają niniejszemu rozporządzeniu, w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 46 ust. 2 lit. f). Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązania – w drodze umowy lub poprzez inne prawnie wiążące instrumenty – do stosowania tych odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.	**N**			
	3. Certyfikacja jest dobrowolna, a proces jej uzyskania musi być przejrzysty.	**T**	**Art. 15 ust 1 i ust. 2**	**Art. 15.** 1. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, zwanej dalej „certyfikacją”, dokonuje Prezes Urzędu i podmiot certyfikujący, na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek. 2. Certyfikacja jest dokonywania na zasadach określonych w rozporządzeniu 2016/679.	
	4. Certyfikacja przewidziana w niniejszym artykule nie wpływa na spoczywający na administratorze lub podmiocie przetwarzającym obowiązek przestrzegania niniejszego rozporządzenia i pozostaje bez uszczerbku dla zadań i uprawnień organów nadzorczych właściwych na mocy art. 55 lub 56.	**N**			
	5. Certyfikacji przewidzianej w niniejszym artykule dokonują podmioty certyfikujące, o których mowa w art. 43, lub dokonuje jej właściwy organ nadzorczy – na podstawie kryteriów zatwierdzonych przez niego zgodnie z art. 58 ust. 3 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63. W przypadku gdy kryteria są zatwierdzane przez Europejską Radę Ochrony Danych, może to skutkować wspólną certyfikacją, europejskim znakiem jakości ochrony danych.	**T**	**Art. 15 ust. 1 Art. 16**	**Art. 15.** 1. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, zwanej dalej „certyfikacją”, dokonuje Prezes Urzędu i podmiot certyfikujący, na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek.	

				Art. 16. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679.	
	6. Administrator lub podmiot przetwarzający, którzy poddają swoje przetwarzanie mechanizmowi certyfikacji, udzielają podmiotowi certyfikującemu, o którym mowa w art. 43, lub gdy ma to zastosowanie – właściwemu organowi nadzorczemu wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania, które to informacje i dostęp są niezbędne do przeprowadzenia procedury certyfikacji.	**T**	**Art. 24** **Art. 25**	**Art. 24. 1.** Prezes Urzędu w terminie, o którym mowa w art. 18 ust. 1, a także po dokonaniu certyfikacji jest uprawniony do przeprowadzenia czynności sprawdzających u administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek, w celu oceny spełniania przez ten podmiot kryteriów certyfikacji. 2. Prezes Urzędu zawiadamia podmiot, o którym mowa w ust. 1, o zamiarze przeprowadzenia czynności sprawdzających. 3. Czynności sprawdzające przeprowadza się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia podmiotowi, o którym mowa w ust. 1, zawiadomienia o zamiarze ich przeprowadzenia. Jeżeli czynności sprawdzające nie zostaną przeprowadzone w terminie 30 dni od dnia doręczenia zawiadomienia, ich przeprowadzenie wymaga ponownego zawiadomienia. 4. Czynności sprawdzające przeprowadza się na podstawie imiennego upoważnienia wydanego przez Prezesa Urzędu, które zawiera: 1) imię i nazwisko osoby przeprowadzającej czynności sprawdzające; **2)** oznaczenie administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek; 3) wskazanie podstawy prawnej przeprowadzenia czynności sprawdzających; 4) zakres czynności sprawdzających; 5) datę i miejsce wystawienia imiennego upoważnienia; 6) podpis osoby uprawnionej do wydania upoważnienia w imieniu Prezesa Urzędu. **Art. 25.** 1. Osoba przeprowadzająca czynności	

				sprawdzające jest uprawniona do: 1) wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń w dniach i godzinach pracy administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek; 2) wglądu do dokumentów i informacji mających bezpośredni związek z działalnością objętą certyfikacją; 3) oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych; 4) żądania ustnych lub pisemnych wyjaśnień w sprawach związanych z działalnością objętą certyfikacją. 2. Czynności sprawdzających dokonuje się w obecności administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek lub osoby przez niego upoważnionej. 3. Z czynności sprawdzających sporządza się protokół i przedstawia administratorowi, podmiotowi przetwarzającemu, producentowi albo podmiotowi wprowadzającemu usługę lub produkt na rynek. Przepis art. 88 stosuje się odpowiednio.	
	7. Certyfikacji administratora lub podmiotu przetwarzającego udziela się na maksymalny okres 3 lat; certyfikację można przedłużyć na tych samych warunkach, o ile nadal spełnione są stosowne wymogi. W stosownym przypadku organy certyfikujące, o których mowa w art. 43, lub właściwy organ nadzorczy cofają certyfikację, jeżeli jej wymogi nie są spełnione lub przestały być spełniane.	**T**	**Art. 22**	**Art. 22**. 1. W okresie, na jaki została dokonana certyfikacja, podmiot, któremu wydano certyfikat, jest obowiązany spełniać kryteria certyfikacji obowiązujące na dzień jego wydania. 2. Prezes Urzędu albo podmiot certyfikujący cofa certyfikację w przypadku stwierdzenia, że podmiot, któremu wydano certyfikat nie spełnia lub przestał spełniać kryteria certyfikacji. 3. Cofnięcie certyfikacji przez Prezesa Urzędu następuje w drodze decyzji.	
	8. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków.	**N**			

Art. 43	**Podmiot certyfikujący** 1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 podmiot certyfikujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych dokonuje certyfikacji i jej przedłużenia po poinformowaniu organu nadzorczego w celu umożliwienia mu w razie potrzeby wykonywania uprawnień na mocy art. 58 ust. 2 lit. h) -. Państwa członkowskie zapewniają akredytację tych podmiotów certyfikujących przez: a) organ nadzorczy właściwy zgodnie z art. 55 lub 56; lub b) krajową jednostkę akredytującą określoną zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 - zgodnie z EN-ISO/IEC 17065/2012 - oraz zgodnie z dodatkowymi wymogami określonymi przez organ nadzorczy właściwy zgodnie z. 55 lub 56.	**T**	**Art. 12 ust. 1**	**Art. 12**. 1. Akredytacji podmiotów ubiegających się o uprawnienie do certyfikacjiw zakresie ochrony danych osobowych, o której mowa w art. 43 rozporządzenia 2016/679, zwanej dalej „akredytacją", udziela Polskie Centrum Akredytacji.	
	2. Podmioty certyfikujące, o których mowa w ust. 1, zostają akredytowane zgodnie z tym ustępem w przypadku gdy: a) w sposób satysfakcjonujący wykazały właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie podlegającej certyfikacji; b) zobowiązały się do przestrzegania kryteriów, o których mowa w art. 42 ust. 5 i które zostały zatwierdzone przez organ nadzorczy właściwy zgodnie z art. 55 lub 56 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63; c) dysponują procedurami wydawania, okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych; d) dysponują procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie warunków certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający, oraz które zapewniają przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz e) w sposób satysfakcjonujący wykażą właściwemu organowi nadzorczemu, że ich zadania i obowiązki nie powodują konfliktu interesów.	**N**			
	3. Akredytacja podmiotów certyfikujących, o których mowa w ust. 1 i 2 niniejszego artykułu, jest dokonywana na podstawie kryteriów zatwierdzonych przez organ nadzorczy właściwy zgodnie z art. 55 lub 56 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63. W przypadku akredytacji na mocy ust. 1 lit. c) niniejszego artykułu wymogi te są uzupełnieniem wymogów przewidzianych w rozporządzeniu (WE) nr 765/2008 oraz przepisów technicznych określających metody i procedury podmiotów certyfikujących.	**T**	**Art. 13**	**Art. 13**. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria akredytacji, o których mowa w art. 43 ust. 3 rozporządzenia 2016/679.	
	4. Podmioty certyfikujące, o których mowa w ust. 1, są odpowiedzialne za dokonanie właściwej oceny przed udzieleniem lub cofnięciem certyfikacji, bez uszczerbku dla spoczywającego na administratorze lub podmiocie przetwarzającym obowiązku przestrzegania niniejszego rozporządzenia. Akredytacji udziela się na maksymalny okres pięciu lat; można ją przedłużyć na tych samych warunkach, o ile podmiot certyfikujący spełnia wymogi określone w niniejszym artykule.	**N**			

	5. Podmioty certyfikujące, o których mowa w ust. 1, przedstawiają właściwemu organowi nadzorczemu powody udzielenia lub cofnięcia żądanej certyfikacji.	**T**	**Art. 19**	**Art. 19**. Przed udzieleniem certyfikacji podmiot certyfikujący informuje Prezesa Urzędu o planowanym dokonaniu albo odmowie dokonania certyfikacji.	
	6. Organ nadzorczy w łatwo dostępny sposób podaje do wiadomości publicznej wymogi, o których mowa w ust. 3 niniejszego artykułu, oraz kryteria, o których mowa w art. 42 ust. 5. Organy nadzorcze przekazują te wymogi i kryteria także Europejskiej Radzie Ochrony Danych. Gromadzi ona w rejestrze wszystkie mechanizmy certyfikacji oraz znaki jakości w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków.	**T**	**Art.13** **Art. 16**	**Art. 13**. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria akredytacji, o których mowa w art. 43 ust. 3 rozporządzenia 2016/679. **Art. 16**. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679.	
	7. Bez uszczerbku dla rozdziału VIII właściwy organ nadzorczy lub krajowa jednostka akredytująca cofają akredytację podmiotu certyfikującego zgodnie z ust. 1 niniejszego artykułu, w przypadku gdy podmiot ten nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania podejmowane przez podmiot certyfikujący naruszają niniejsze rozporządzenie.	**N**			
	8. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 92 w celu doprecyzowania wymogów, które uwzględnia się w przypadku mechanizmów certyfikacji w dziedzinie ochrony danych, o których mowa w art. 42 ust. 1.	**N**			
	9. Komisja może przyjąć akty wykonawcze określające techniczne standardy mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposoby upowszechniania i uznawania tych mechanizmów certyfikacji oraz znaków jakości i oznaczeń. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.	**N**			
ROZDZIAŁ V **Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych**					
Art. 44	**Ogólna zasada przekazywania** Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy - z zastrzeżeniem innych przepisów niniejszego rozporządzenia - administrator i podmiot przetwarzający spełnią warunki określone w niniejszym rozdziale, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu.	**N**			
Art. 45	**Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony**	**N**			

	1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia. 2. Oceniając, czy stopień ochrony jest odpowiedni, Komisja uwzględnia w szczególności następujące elementy: a) praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo - zarówno ogólne, jak i sektorowe - w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia; b) istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub w stosunku do organizacji międzynarodowej, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych - w tym posiadające odpowiednie uprawnienia do egzekwowania przestrzegania przepisów - pomagać i doradzać osobom, których dane dotyczą, w toku wykonywania przysługujących im praw, a także współpracować z organami nadzorczymi państw członkowskich; oraz c) międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne obowiązki wynikające z prawnie wiążących konwencji lub instrumentów oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych. 3. Po dokonaniu oceny, czy stopień ochrony jest odpowiedni, Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu. W akcie wykonawczym przewiduje się mechanizm okresowego przeglądu - przynajmniej raz na cztery lata - podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej. W akcie wykonawczym zostaje określony terytorialny i sektorowy zakres jego zastosowania, a gdy ma to zastosowanie wskazany zostaje organ nadzorczy lub organy nadzorcze, o których mowa w ust. 2 lit. b) niniejszego artykułu. Akt wykonawczy zostaje przyjęty zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2. 4. Komisja na bieżąco monitoruje zmiany w państwach trzecich i organizacjach międzynarodowych mogące wpłynąć na obowiązywanie decyzji				

	przyjętych na mocy ust. 3 niniejszego artykułu oraz decyzji przyjętych na podstawie art. 25 ust. 6 dyrektywy 95/46/WE. 5. Jeżeli dostępne informacje na to wskazują, w szczególności po przeglądzie, o którym mowa w ust. 3 niniejszego artykułu, Komisja przyjmuje decyzję stwierdzającą, że państwo trzecie - lub terytorium lub jeden lub więcej określonych sektorów w tym państwie trzecim - lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu, i w niezbędnym zakresie uchyla, zmienia lub zawiesza decyzję, o której mowa w ust. 3 niniejszego artykułu, w drodze aktów wykonawczych bez mocy wstecznej. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2. W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja przyjmuje zgodnie z procedurą, o której mowa w art. 93 ust. 3 akty wykonawcze mające natychmiastowe zastosowanie. 6. Komisja podejmuje konsultacje z państwem trzecim lub organizacją międzynarodową w celu zaradzenia sytuacji będącej przyczyną decyzji przyjętej na mocy ust. 5. 7. Decyzja przyjęta na mocy ust. 5 niniejszego artykułu pozostaje bez uszczerbku dla przekazywania danych osobowych do danego państwa trzeciego, terytorium lub określonego sektora lub określonych sektorów w tym państwie trzecim lub do danej organizacji międzynarodowej na mocy art. 46-49. 8. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* i na swojej stronie internetowej wykaz państw trzecich, terytoriów i określonych sektorów w państwie trzecim oraz organizacji międzynarodowych, co do których przyjęła decyzję stwierdzającą odpowiedni stopień ochrony lub jego brak. 9. Decyzje przyjęte przez Komisję na mocy art. 25 ust. 6 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia decyzją Komisji przyjętą zgodnie z ust. 3 lub 5 niniejszego artykułu.				
Art. 46	**Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń** 1. W razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. 2. Odpowiednie zabezpieczenia, o których mowa w ust. 1, można zapewnić - bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego - za pomocą: a) prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi; b) wiążących reguł korporacyjnych zgodnie z art. 47;	**N** **N** **T**	**Art. 57 pkt 1**	**Art. 57**. Prezes Urzędu w drodze decyzji: 1) zatwierdza wiążące reguły korporacyjne, o	

				których mowa w art. 47 rozporządzenia 2016/679;	
	c) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;	**N**			
	d) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;	**T**	**Art. 54 ust 1 pkt 3**	**Art. 54**. 1. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej: 3) przyjęte standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit d rozporządzenia 2016/679;	
	e) zatwierdzonego kodeksu postępowania zgodnie z art. 40 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą; lub	**T**	**Art. 27**	**Art. 27**. 1. Kodeks postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, zwany dalej „kodeksem postępowania" jest opracowywany, opiniowany i zatwierdzany na zasadach określonych w tym rozporządzeniu. 2. Kodeks postępowania przed przekazaniem do zatwierdzenia Prezesowi Urzędu podlega konsultacjom z zaineresowanymi podmiotami.	
	f) zatwierdzonego mechanizmu certyfikacji zgodnie z art. 42 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.	**N**			
	3. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w ust. 1, można także zapewnić w szczególności za pomocą: a) klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej; lub b) postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.	**T**	**Art. 57 pkt 2**	**Art. 57**. Prezes Urzędu w drodze decyzji: 2) udziela zezwolenia, o którym mowa w art. 46 ust. 3 rozporządzenia 2016/679.	
	4. W przypadkach, o których mowa w ust. 3 niniejszego artykułu, organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.	**N**			
	5. Zezwolenia wydane przez państwo członkowskie lub organ nadzorczy na podstawie art. 26 ust. 2 dyrektywy 95/46/WE zachowują ważność do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby przez ten organ. Decyzje	**N**			

	przyjęte przez Komisję na mocy art. 26 ust. 4 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby decyzją Komisji przyjętą zgodnie z ust. 2 niniejszego artykułu.				
Art. 47	**Wiążące reguły korporacyjne** 1. Właściwy organ nadzorczy zatwierdza wiążące reguły korporacyjne zgodnie z mechanizmem spójności przewidzianym w art. 63, pod warunkiem że: a) są one prawnie wiążące oraz mają zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w tym ich pracowników, i są przez każdego z tych członków egzekwowane; b) wyraźnie przyznają osobom, których dane dotyczą, egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych; oraz c) spełniają wymogi określone w ust. 2. 2. W wiążących regułach korporacyjnych, o których mowa w ust. 1, określone zostają co najmniej: a) struktura i dane kontaktowe odnośnej grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i każdego z jej członków; b) jednorazowe lub wielokrotne przekazanie danych, w tym kategorie danych osobowych, rodzaj przetwarzania i jego cele, rodzaje osób, których dane dotyczą, oraz nazwa danego państwa trzeciego lub danych państw trzecich; c) ich prawnie wiążący charakter, wewnętrzny i zewnętrzny; d) zastosowanie ogólnych zasad ochrony danych - w szczególności ograniczenia celu, minimalizacji danych, ograniczonych okresów przechowywania, jakości danych, uwzględnianie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, podstawa prawna przetwarzania, przetwarzanie szczególnych kategorii danych osobowych, środki zapewniające bezpieczeństwo danych, wymogi w zakresie dalszego przekazywania podmiotom niezwiązanym wiążącymi regułami korporacyjnymi; e) prawa osób, których dane dotyczą, w związku z przetwarzaniem oraz sposoby wykonywania tych praw, w tym z prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu - w tym profilowaniu - zgodnie z art. 22, prawa do wnoszenia skarg do właściwego organu nadzorczego i właściwych sądów państw członkowskich zgodnie z art. 79 oraz prawa do środka zaskarżenia, a w stosownych przypadkach - odszkodowania za naruszenie wiążących reguł korporacyjnych; f) przyjęcie przez administratora lub podmiot przetwarzający posiadających jednostki organizacyjnej na terytorium państwa członkowskiego odpowiedzialności prawnej za naruszenie wiążących reguł korporacyjnych przez odnośnego członka niemającego jednostki organizacyjne w Unii; administrator lub podmiot przetwarzający są zwolnieni z tej odpowiedzialności - w całości lub w części - wyłącznie, gdy udowodni, że członek ten nie ponosi odpowiedzialności za wydarzenie, które doprowadziło do powstania szkody; g) sposób, w jaki osobom, których dane dotyczą, podaje się - oprócz	**T** **N**	**Art. 57 pkt 1**	**Art. 57**. Prezes Urzędu w drodze decyzji: 1) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 rozporządzenia 2016/679;	

	informacji, o których mowa w art. 13 i 14 - informacje o wiążących regułach korporacyjnych, w szczególności o postanowieniach, o których mowa w lit. d), e) i f) niniejszego ustępu; h) zadania inspektora ochrony danych wyznaczonego zgodnie z art. 37 lub innej osoby lub podmiotu odpowiedzialnych za monitorowanie przestrzegania wiążących reguł korporacyjnych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz monitorowanie szkoleń i rozpatrywanie skarg; i) procedury dotyczące skarg; j) stosowane w grupie przedsiębiorstw lub w grupie przedsiębiorców prowadzących wspólną działalność gospodarczą mechanizmy zapewniające weryfikację przestrzegania wiążących reguł korporacyjnych. Mechanizmy takie obejmują audyty w zakresie ochrony danych oraz metody zapewniania działań naprawczych mających chronić prawa osób, których dane dotyczą. Wyniki takiej weryfikacji powinny być przekazywane osobie lub podmiotowi, o których mowa w lit. h), oraz zarządowi przedsiębiorstwa sprawującego kontrolę w grupie przedsiębiorstw lub organowi kierującemu grupą przedsiębiorców prowadzących wspólną działalność gospodarczą i powinny być dostępne na żądanie właściwego organu nadzorczego; k) mechanizmy zgłaszania i rejestrowania zmian w zasadach i zgłaszania tych zmian organowi nadzorczemu; l) mechanizm współpracy z organem nadzorczym zapewniający przestrzeganie zasad przez wszystkich członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w szczególności poprzez udostępnianie organowi nadzorczemu wyników weryfikacji środków, o której mowa w lit. j); m) mechanizm zgłaszania właściwemu organowi nadzorczemu wszelkich wymogów prawnych, którym podlega w państwie trzecim członek grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i które mogą mieć istotny niekorzystny wpływ na gwarancje przewidziane w wiążących regułach korporacyjnych; oraz n) właściwe szkolenia z zakresu ochrony danych dla personelu mającego stały lub regularny dostęp do danych osobowych. 3. Komisja może określić format i procedury wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi dotyczących wiążących reguł korporacyjnych w rozumieniu niniejszego artykułu. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.	**N**			
Art. 48	**Przekazywanie lub ujawnienie niedozwolone na mocy prawa Unii** Wyrok sądu lub trybunału oraz decyzja organu administracyjnego państwa trzeciego wymagające od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych mogą zostać uznane lub być egzekwowalne wyłącznie, gdy opierają się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią lub państwem członkowskim, bez uszczerbku dla innych podstaw przekazania na mocy niniejszego rozdziału.	**N**			

Art. 49	**Wyjątki w szczególnych sytuacjach** 1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust. 3 lub braku odpowiednich zabezpieczeń określonych w art. 46, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że: a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi - ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń - może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę; b) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą; c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną; d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego; e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń; f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub g) przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes - ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego. Jeżeli przekazanie nie może się opierać na art. 45 ani 46, w tym na przepisach dotyczących wiążących reguł korporacyjnych, i nie ma zastosowania żaden z wyjątków mających zastosowanie w szczególnych sytuacjach zgodnie z akapitem pierwszym niniejszego ustępu, przekazanie do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie, gdy przekazanie nie jest powtarzalne, dotyczy tylko ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą a administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych. Administrator informuje organ nadzorczy o przekazaniu. Poza informacjami, o których mowa w art. 13 i 14, administrator podaje osobie, której dane dotyczą, także informacje o przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez niego. 2. Przekazanie na mocy ust. 1 akapit pierwszy lit. g) nie obejmuje całości danych osobowych ani całych kategorii danych osobowych zawartych w rejestrze. Jeżeli rejestr jest dostępny dla osób mających prawnie uzasadniony interes, przekazanie następuje wyłącznie na żądanie tych osób lub gdy mają one być odbiorcami. 3. Ust. 1 akapit pierwszy lit. a), b), c) oraz ust. 1 akapit drugi tego ustępu nie mają	**N**			

	zastosowania do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych. 4. Interes publiczny, o którym mowa w ust. 1 akapit pierwszy lit. d), musi być uznany w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator. 5. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony prawo Unii lub prawo państwa członkowskiego może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Państwa członkowskie powiadamiają Komisję o takich przepisach. 6. Administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie zabezpieczenia, o których mowa w ust. 1 akapit drugi niniejszego artykułu, w rejestrach, o których mowa w art. 30.				
Art. 50	**Międzynarodowa współpraca na rzecz ochrony danych osobowych** Komisja i organy nadzorcze podejmują wobec państw trzecich i organizacji międzynarodowych odpowiednie działania na rzecz: a) wypracowania mechanizmów współpracy międzynarodowej ułatwiających skuteczne egzekwowanie przepisów o ochronie danych osobowych; b) zapewnienia wzajemnej pomocy międzynarodowej w egzekwowaniu przepisów o ochronie danych osobowych, w tym poprzez powiadomienia, przekazywanie skarg, pomoc w postępowaniu wyjaśniającym oraz wymianę informacji - z zastrzeżeniem odpowiednich zabezpieczeń ochrony danych osobowych i innych podstawowych praw i wolności; c) włączenia stosownych podmiotów, których sprawa dotyczy, w dyskusję i działalność mające na celu upowszechnianie międzynarodowej współpracy w dziedzinie egzekwowania przepisów o ochronie danych osobowych; d) upowszechniania wymiany i dokumentowania przepisów i praktyk w dziedzinie ochrony danych osobowych, w tym konfliktów jurysdykcyjnych z państwami trzecimi.	**N**			
ROZDZIAŁ VI **Niezależne organy nadzorcze**					
Sekcja 1 **Niezależny status**					
Art. 51	**Organ nadzorczy** 1. Każde państwo członkowskie zapewnia, by za monitorowanie stosowania niniejszego rozporządzenia odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii (zwany dalej "organem nadzorczym").	**T**	**Art. 34 ust. 1 i 2**	**Art. 34.** 1. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych. 2. Prezes Urzędu jest organem nadzorczym w rozumieniu rozporządzenia 2016/679, w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych	

	2. Każdy organ nadzorczy przyczynia się do spójnego stosowania niniejszego rozporządzenia w całej Unii. W tym celu organy nadzorcze współpracują ze sobą i z Komisją zgodnie z rozdziałem VII. 3. Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, państwo to wskazuje, który z nich ma reprezentować te organy w Europejskiej Radzie Ochrony Danych, oraz ustala mechanizm zapewniający przestrzeganie przez pozostałe organy przepisów o mechanizmie spójności, o którym mowa w art. 63. 4. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o przepisach przyjętych na mocy niniejszego rozdziału, a następnie niezwłocznie o każdej kolejnej zmianie mającej na nie wpływ.			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, str. 89) oraz w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) (Dz. Urz. UE L 135 z 24.5.2016, str. 53).	
Art. 52	**Niezależność** 1. Każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem działa w sposób w pełni niezależny. 2. Członek lub członkowie każdego organu nadzorczego podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem pozostają wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują.	**T**	**Art. 34 ust. 3, ust. 5 i ust. 9** **Art. 38 ust. 1**	**Art. 34.** 3. Prezesa Urzędu powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu Rzeczypospolitej Polskiej. 5. Prezes Urzędu w zakresie wykonywania swoich zadań podlega tylko ustawie. 9. Prezes Urzędu może zostać odwołany przed upływem kadencji, wyłącznie w przypadku, gdy: 1) zrzekł się stanowiska; 2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby stwierdzonej orzeczeniem lekarskim; 3) sprzeniewierzył się ślubowaniu; 4) został skazany prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego; 5) został pozbawiony praw publicznych. **Art. 38.** 1. Prezes Urzędu nie może być bez uprzedniej zgody Sejmu pociągnięty do odpowiedzialności karnej ani pozbawiony wolności, z zastrzeżeniem ust. 2.	

	3. Członek lub członkowie każdego organu nadzorczego powstrzymują się od wszelkich czynności sprzecznych ze swoimi obowiązkami i podczas swojej kadencji nie podejmują żadnego zajęcia zarobkowego ani niezarobkowego sprzecznego z tymi obowiązkami.	**T**	**Art. 37**	**Art. 37**. 1. Prezes Urzędu oraz jego zastępcy nie mogą zajmować innego stanowiska, z wyjątkiem stanowiska dydaktycznego, naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, ani wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu. 2. Prezes Urzędu oraz jego zastępcy nie mogą należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.	
	4. Każde państwo członkowskie zapewnia, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień, w tym w zakresie wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych. 5. Każde państwo członkowskie zapewnia, by każdy organ nadzorczy wybierał i posiadał własny personel, działający pod wyłącznym kierownictwem członka lub członków danego organu nadzorczego.	**T**	**Art. 46**	**Art. 46**. 1. Prezes Urzędu wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych zwanego dalej „Urzędem". 2. W przypadkach uzasadnionych charakterem i liczbą spraw z zakresu ochrony danych osobowych na danym terenie, Prezes Urzędu może w ramach Urzędu tworzyć jednostki zamiejscowe Urzędu. 3. Prezes Urzędu, w drodze zarządzenia, nadaje statut Urzędowi, określając: 1) organizację wewnętrzną Urzędu, 2) zakres zadań swoich zastępców, 3) zakres zadań i tryb pracy komórek organizacyjnych Urzędu – mając na uwadze stworzenie optymalnych warunków organizacyjnych do prawidłowej realizacji zadań Urzędu.	
	6. Każde państwo członkowskie zapewnia, by każdy organ nadzorczy podlegał kontroli finansowej w sposób nienaruszający jego niezależności oraz dysponował odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.	**N**			
Art. 53	**Ogólne warunki dotyczące członków organu nadzorczego** 1. 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.	**T**	**Art. 34 ust. 3** **Art. 36 ust. 1**	**Art. 34**. 3. Prezesa Urzędu powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu Rzeczypospolitej Polskiej **Art. 36.** 1. Prezes Urzędu może powołać do trzech zastępców.	

	2. Każdy członek musi posiadać kwalifikacje, doświadczenie i umiejętności - w szczególności w dziedzinie ochrony danych osobowych - potrzebne do wypełniania swoich obowiązków i wykonywania swoich uprawnień.	**T**	**Art. 34 ust. 4**	**Art. 34.** 4. Na stanowisko Prezesa Urzędu może być powołana osoba, która: 1) jest obywatelem polskim; 2) posiada wyższe wykształcenie; 3) wyróżnia się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych; 4) korzysta z pełni praw publicznych; 5) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe; 6) posiada nieposzlakowaną opinię.	
	3. W razie upływu kadencji, rezygnacji lub przymusowego pozbawienia funkcji członek organu przestaje pełnić swoje obowiązki zgodnie z prawem danego państwa członkowskiego. 4. Członek może zostać odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki niezbędne do pełnienia obowiązków.	**T**	**Art. 34 ust 8 - 10**	**Art. 34**. 8. Kadencja Prezesa Urzędu wygasa z chwilą jego śmierci, odwołania lub utraty obywatelstwa polskiego. 9. Prezes Urzędu może zostać odwołany przed upływem kadencji, wyłącznie w przypadku, gdy: 1) zrzekł się stanowiska; 2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby stwierdzonej orzeczeniem lekarskim; 3) sprzeniewierzył się ślubowaniu; 4) został skazany prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego; 5) został pozbawiony praw publicznych. 10. W przypadku odwołania lub wygaśnięcia kadencji Prezesa Urzędu jego obowiązki pełni zastępca Prezesa Urzędu wskazany przez Marszałka Sejmu.	

Art. 54	**Zasady ustanawiania organu nadzorczego** 1. Każde państwo członkowskie określa w swoich przepisach prawnych wszystkie poniższe elementy:				
	a) ustanowienie każdego z organów nadzorczych;	**T**	**Art. 34 ust. 1 – 2**	**Art. 34.** 1. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych. 2. Prezes Urzędu jest organem nadzorczym w rozumieniu rozporządzenia 2016/679, w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016, str. 89) oraz w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) (Dz. Urz. UE L 135 z 24.5.2016, str. 53).	
	b) kwalifikacje i warunki wyboru wymagane do powołania na stanowisko członka każdego z organów nadzorczych;	**T**	**Art. 34 ust. 4**	**Art. 34.** 4. Na stanowisko Prezesa Urzędu może być powołana osoba, która: 1) jest obywatelem polskim; 2) posiada wyższe wykształcenie; 3) wyróżnia się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych; 4) korzysta z pełni praw publicznych; 5) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe; 6) posiada nieposzlakowaną opinię.	
	c) zasady i procedury powoływania członka lub członków każdego z organów nadzorczych;	**N**			
	d) okres kadencji członka lub członków każdego z organów nadzorczych - nie krótszy niż cztery lata, z wyjątkiem pierwszej kadencji po dniu 24 maja 2016 r., która może częściowo trwać krócej, jeżeli jest to niezbędne, aby chronić niezależność organu nadzorczego w drodze procedury stopniowej wymiany członków;	**T**	**Art. 34 ust. 6**	**Art. 34.** 6. Kadencja Prezesa Urzędu trwa 4 lata licząc od dnia złożenia ślubowania. Prezes Urzędu po upływie kadencji wykonuje swoje obowiązki do czasu objęcia stanowiska przez nowego Prezesa Urzędu.	

	e) czy członek lub członkowie każdego z organów nadzorczych mogą zostać powołani ponownie, a jeżeli tak - na ile kadencji;	**T**	**Art. 34 ust. 7**	**Art. 34.** 7. Ta sama osoba nie może być Prezesem Urzędu więcej niż przez dwie kadencje.	
	f) zasady regulujące obowiązki członka lub członków oraz personelu każdego z organów nadzorczych, zakaz podejmowania działań, zajęć i czerpania korzyści - w trakcie kadencji oraz po jej zakończeniu - sprzecznych z tymi zobowiązaniami, a także przepisy regulujące ustanie stosunku pracy.	**T**	**Art. 37**	**Art. 37**. 1. Prezes Urzędu oraz jego zastępcy nie mogą zajmować innego stanowiska, z wyjątkiem stanowiska dydaktycznego, naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej, ani wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami Prezesa Urzędu. 2. Prezes Urzędu oraz jego zastępcy nie mogą należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.	
	2. Członek lub członkowie oraz personel każdego z organów nadzorczych podlegają zgodnie z prawem Unii lub prawem państwa członkowskiego obowiązkowi zachowania tajemnicy służbowej - w trakcie kadencji oraz po jej zakończeniu - w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wypełniania zadań lub wykonywania swoich uprawnień. Obowiązek zachowania tajemnicy służbowej w trakcie ich kadencji dotyczy w szczególności sytuacji, w których osoby fizyczne zgłaszają naruszenia niniejszego rozporządzenia.	**T**	**Art. 47**	**Art. 47**. 1. Prezes Urzędu, zastępcy Prezesa Urzędu a także pracownicy Urzędu są obowiązani zachować w tajemnicy informacje, o których dowiedzieli się w związku z wykonywaniem czynności służbowych. 2. Obowiązek zachowania w tajemnicy informacji, o których mowa w ust. 1, nie może być ograniczony w czasie i trwa także po zakończeniu kadencji albo zatrudnienia.	
Sekcja 2 **Właściwość, zadania i uprawnienia**					
Art. 55	**Właściwość** 1. Każdy organ nadzorczy jest właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z niniejszym rozporządzeniem na terytorium swojego państwa członkowskiego. 2. Jeżeli przetwarzania dokonują organy publiczne lub podmioty prywatne działające na podstawie art. 6 ust. 1 lit. c) lub e), organem właściwym jest organ	**T**	**Art. 34**	**Art. 34.** 1. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych. 2. Prezes Urzędu jest organem nadzorczym w rozumieniu rozporządzenia 2016/679, w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych	

	nadzorczy danego państwa członkowskiego. W takich przypadkach art. 56 nie ma zastosowania. 3. Organy nadzorcze nie są właściwe do nadzorowania operacji przetwarzania dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości.			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, str. 89) oraz w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) (Dz. Urz. UE L 135 z 24.5.2016, str. 53).	
Art. 56	**Właściwość wiodącego organu nadzorczego** 1. Bez uszczerbku dla art. 55 organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy - zgodnie z procedurą przewidzianą w art. 60 - względem transgranicznego przetwarzania dokonywanego przez tego administratora lub ten podmiot przetwarzający. 2. W drodze wyjątku od ust. 1 każdy organ nadzorczy jest właściwy do rozpatrzenia skargi, którą do niego wniesiono, lub zajęcia się ewentualnym naruszeniem niniejszego rozporządzenia, jeżeli sprawa dotyczy wyłącznie jednostki organizacyjnej w jego państwie członkowskim lub znacznie wpływa na osoby, których dane dotyczą, wyłącznie w jego państwie członkowskim. 3. W przypadkach, o których mowa w ust. 2 niniejszego artykułu, organ nadzorczy niezwłocznie informuje o danej sprawie wiodący organ nadzorczy. W terminie trzech tygodni od otrzymania informacji wiodący organ nadzorczy postanawia, czy zajmie się daną sprawą zgodnie z procedurą przewidzianą w art. 60, uwzględniając, czy w państwie członkowskim, którego organ nadzorczy przekazał mu informacje, znajduje się jednostka organizacyjna administratora lub podmiotu przetwarzającego. 4. Jeżeli wiodący organ nadzorczy postanowi zająć się daną sprawą, zastosowanie ma procedura przewidziana w art. 60. Organ nadzorczy, który przekazał informacje wiodącemu organowi nadzorczemu, może przedłożyć temu organowi projekt decyzji. Wiodący organ nadzorczy w jak największym stopniu uwzględnia ten projekt, przygotowując projekt decyzji, o którym mowa w art. 60 ust. 3. 5. Jeżeli wiodący organ nadzorczy postanowi nie zajmować się daną sprawą, sprawą zajmuje się - zgodnie z art. 61 i 62 - organ nadzorczy, który przekazał informacje wiodącemu organowi nadzorczemu. 6. Administrator lub podmiot przetwarzający komunikują się w sprawie dokonywanego przez nich transgranicznego przetwarzania jedynie z wiodącym organem nadzorczym.	**N**			
Art. 57	**Zadania** 1. Bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia każdy organ nadzorczy na swoim terytorium:				

	a)	monitoruje i egzekwuje stosowanie niniejszego rozporządzenia;	**N**			
	b)	upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci;	**N**			
	c)	doradza, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem;	**T**	**Art. 52**	**Art. 52.** Założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu.	
	d)	upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia;	**N**			
	e)	udziela osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących im na mocy niniejszego rozporządzenia, a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi innych państw członkowskich;	**N**			
	f)	rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym;	**T**	**Art. 60**	**Art. 60.** Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", jest prowadzone przez Prezesa Urzędu.	
	g)	współpracuje z innymi organami nadzorczymi, w tym dzieli się informacjami oraz świadczy wzajemną pomoc, w celu zapewnienia spójnego stosowania i egzekwowania niniejszego rozporządzenia;	**N**			
	h)	prowadzi postępowania w sprawie stosowania niniejszego rozporządzenia, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;	**T**	**Art. 60**	**Art. 60.** Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", jest prowadzone przez Prezesa Urzędu.	
	i)	monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych;	**N**			
	j)	przyjmuje standardowe klauzule umowne, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d);	**T**	**Art. 54 ust. 1 pkt 1 i 3**	**Art. 54. 1.** Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej: 1) standardowe klauzule umowne, o których mowa w art. 28 ust. 8 rozporządzenia 2016/679; 3) przyjęte standardowe klauzule ochrony danych,	

				o których mowa w art. 46 ust. 2 lit d rozporządzenia 2016/679;	
	k) ustanawia i prowadzi wykaz związany z wymogiem dokonania oceny skutków dla ochrony danych na mocy art. 35 ust. 4;	**T**	**Art. 55**	**Art. 55**. 1. Prezes Urzędu: 1) ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679; 2) może ogłosić w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych niewymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 5 rozporządzenia 2016/679. 2. Komunikat, o którym mowa w ust. 1, ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.	
	l) udziela zaleceń, o których mowa w art. 36 ust. 2, dotyczących operacji przetwarzania;	**N**			
	m) zachęca do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia, na mocy art. 40 ust. 5;	**T**	**Art. 27 ust. 1 i 2**	**Art. 27**. 1. Kodeks postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, zwany dalej „kodeksem postępowania” jest opracowywany, opiniowany i zatwierdzany na zasadach określonych w tym rozporządzeniu. 2. Kodeks postępowania przed przekazaniem do zatwierdzeniem Prezesowi Urzędu podlega konsultacjom z zaineresowanymi podmiotami.	
	n) zachęca do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny zgodnie z art. 42 ust. 1, a także zatwierdza kryteria certyfikacji zgodnie z art. 42 ust. 5;	**N**			

	o) gdy ma to zastosowanie - zgodnie z art. 42 ust. 7 dokonuje okresowego przeglądu udzielonych certyfikacji;	**T**	**Art. 22** **Art. 24 ust. 1**	**Art. 22**. 1. W okresie, na jaki została dokonana certyfikacja, podmiot, któremu wydano certyfikat, jest obowiązany spełniać kryteria certyfikacji obowiązujące na dzień jego wydania. 2. Prezes Urzędu albo podmiot certyfikujący cofa certyfikację w przypadku stwierdzenia, że podmiot, któremu wydano certyfikat nie spełnia lub przestał spełniać kryteria certyfikacji. 3. Cofnięcie certyfikacji przez Prezesa Urzędu następuje w drodze decyzji. **Art. 24. 1.** Prezes Urzędu w terminie, o którym mowa w art. 18 ust. 1, a także po dokonaniu certyfikacji jest uprawniony do przeprowadzenia czynności sprawdzających u administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek, w celu oceny spełniania przez ten podmiot kryteriów certyfikacji.	
	p) opracowuje i publikuje kryteria akredytacji podmiotu monitorującego kodeksy postępowania na mocy art. 41 oraz podmiotu certyfikującego na mocy art. 43;	**T**	**Art. 28** **Art. 16**	**Art. 28.** Przestrzeganie zatwierdzonego kodeksu postępowania, monitoruje podmiot akredytowany przez Prezesa Urzędu na zasadach określonych w art. 41 rozporządzenia 2016/679. **Art. 16**. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679.	
	q) akredytuje podmiot monitorujący kodeksy postępowania na mocy art. 41 oraz podmiot certyfikujący na mocy art. 43;	**T**	**Art. 28**	**Art. 28.** Przestrzeganie zatwierdzonego kodeksu postępowania, monitoruje podmiot akredytowany przez Prezesa Urzędu na zasadach określonych w art. 41 rozporządzenia 2016/679.	
	r) wydaje zezwolenia na klauzule umowne i przepisy, o których mowa w art. 46 ust. 3;	**T**	**Art.57 pkt 2**	**Art. 57**. Prezes Urzędu w drodze decyzji: 2) udziela zezwolenia, o którym mowa w art. 46 ust. 3 rozporządzenia 2016/679.	

	s) zatwierdza wiążące reguły korporacyjne na mocy art. 47;	**T**	**Art. 57 pkt 1**	**Art. 57**. Prezes Urzędu w drodze decyzji: 1) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 rozporządzenia 2016/679;	
	t) bierze udział w pracach Europejskiej Rady Ochrony Danych;	**N**			
	u) prowadzi wewnętrzny rejestr naruszeń niniejszego rozporządzenia i działań podjętych zgodnie z art. 58 ust. 2; oraz	**N**			
	v) wypełnia inne zadania związane z ochroną danych osobowych.	**N**			
	2. Każdy organ nadzorczy ułatwia wnoszenie skarg, o których mowa w ust. 1 lit. f), za pomocą takich środków, jak gotowy formularz skargi, który można również wypełnić elektronicznie, co nie wyklucza innych sposobów komunikacji.	**N**			
	3. Każdy organ nadzorczy wypełnia zadania na rzecz osoby, której dane dotyczą, i - gdy ma to zastosowanie - inspektora ochrony danych bezpłatnie.	**N**			
	4. Jeżeli żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swą powtarzalność, organ nadzorczy może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych lub może odmówić podjęcia żądanych działań. Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na organie nadzorczym.	**N**			
Art. 58	**Uprawnienia** 1. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia w zakresie prowadzonych postępowań:				
	a) nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;	**N**			
	b) prowadzenie postępowań w formie audytów ochrony danych;	**N**			
	c) dokonywanie przeglądu udzielonych certyfikacji na mocy art. 42 ust. 7;	**T**	**Art. 24 ust. 1**	**Art. 24. 1.** Prezes Urzędu w terminie, o którym mowa w art. 18 ust. 1, a także po dokonaniu certyfikacji jest uprawniony do przeprowadzenia czynności sprawdzających u administratora, podmiotu przetwarzającego, producenta albo podmiotu	

				wprowadzającego usługę lub produkt na rynek, w celu oceny spełniania przez ten podmiot kryteriów certyfikacji.	
	d) zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia niniejszego rozporządzenia;	**N**			
	e) uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań; f) uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego.	**T**	**Art. 63** **Art. 64** **Art. 84**	**Art. 63.** Prezes Urzędu może żądać od strony przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę. Tłumaczenie dokumentacji strona jest obowiązana wykonać na własny koszt. **Art. 64.** W celu realizacji swoich zadań Prezes Urzędu ma prawo dostępu do informacji objętych tajemnicą prawnie chronioną, chyba że przepisy szczególne stanowią inaczej. **Art. 84. 1.** Kontrolujący ma prawo: 1) wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń; 2) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli; 3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych; 4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego; 5) zlecać sporządzanie ekspertyz i opinii.	
	2. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia naprawcze:				
	a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania;	**N**			

	b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania;	**N**			
	c) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;	**N**			
	d) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;	**N**			
	e) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;	**N**			
	f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;	**N**			
	g) nakazanie na mocy art. 16, 17 i 18 sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;	**N**			
	h) cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;	**T**	**Art. 19**	**Art. 19**. Przed udzieleniem certyfikacji podmiot certyfikujący informuje Prezesa Urzędu o planowanym dokonaniu albo odmowie dokonania certyfikacji.	
	i) zastosowanie, oprócz lub zamiast środków, o których mowa w niniejszym ustępie, administracyjnej kary pieniężnej na mocy art. 83, zależnie od okoliczności konkretnej sprawy;	**N**			
	j) nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.	**N**			
	3. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia w zakresie wydawania zezwoleń i uprawnienia doradcze:				
	a) udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 36;	**N**			
	b) wydawanie, z własnej inicjatywy lub na wniosek, opinii przeznaczonych dla parlamentu narodowego, rządu państwa członkowskiego lub - zgodnie z prawem państwa członkowskiego - innych instytucji i organów oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych;	**N**			

	c) zezwalanie na przetwarzanie zgodnie z art. 36 ust. 5, jeżeli prawo państwa członkowskiego wymaga takiego uprzedniego zezwolenia;	**N**			
	d) opiniowanie i zatwierdzanie projektów kodeksów postępowania zgodnie z art. 40 ust. 5;	**T**	**Art. 27**	**Art. 27. 1.** Kodeks postępowania, o którym mowa w art. 40 rozporządzenia 2016/679, zwany dalej „kodeksem postępowania" jest opracowywany, opiniowany i zatwierdzany na zasadach określonych w tym rozporządzeniu. 2. Kodeks postępowania przed przekazaniem do zatwierdzeniem Prezesowi Urzędu podlega konsultacjom z zaineresowanymi podmiotami. 3. Informację o przeprowadzonych konsultacjach oraz ich wyniku przekazuje się Prezesowi Urzędu wraz z kodeksem postępowania. 4. W przypadku uznania przez Prezesa Urzędu zakresu konsultacji za niewystarczający, wyzywa on podmiot do przeprowadzenia ponownych konsultacji, wskazując ich zakres. 5. Stroną postępowania w sprawie zatwierdzenia kodeksu postępowania jest wyłącznie wnioskodawca występujący o zatwierdzenie tego kodeksu. Przepisu art. 31 ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego, nie stosuje się. 6. Do zmiany zatwierdzonego kodeksu postępowania lub jego rozszerzenia stosuje się ust. 1-5.	
	e) akredytowanie na mocy art. 43 podmiotów certyfikujących;	**N**			
	f) udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji zgodnie z art. 42 ust. 5;	**T**	**Art. 15 i 16**	**Art. 15**. 1. Certyfikacji, o której mowa w art. 42 rozporządzenia 2016/679, zwanej dalej „certyfikacją", dokonuje Prezes Urzędu i podmiot certyfikujący, na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek. 2. Certyfikacja jest dokonywania na zasadach określonych w rozporządzeniu 2016/679. 3. W sprawach dokonywania certyfikacji przez podmiot certyfikujący nieuregulowanych w rozporządzeniu 2016/679 i niniejszej ustawie stosuje się postanowienia umowy cywilnoprawnej zawartej pomiędzy podmiotem certyfikującym a podmiotem ubiegającym się o certyfikację.	

				Art. 16. Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679.	
	g) przyjmowanie standardowych klauzul ochrony danych, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d);	**T**	**Art. 54 ust. 1 pkt 1 i 3**	**Art. 54. 1.** Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej: 1) standardowe klauzule umowne, o których mowa w art. 28 ust. 8 rozporządzenia 2016/679; 3) przyjęte standardowe klauzule ochrony danych, o których mowa w art. 46 ust. 2 lit d rozporządzenia 2016/679;	
	h) zezwalanie na klauzule umowne, o których mowa w art. 46 ust. 3 lit. a);	**N**			
	i) zezwalanie na uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 lit. b);	**T**	**Art. 57 pkt 2**	**Art. 57.** Prezes Urzędu w drodze decyzji: 2) udziela zezwolenia, o którym mowa w art. 46 ust. 3 rozporządzenia 2016/679.	
	j) zatwierdzanie wiążących reguł korporacyjnych na mocy art. 47.	**T**	**Art. 57 pkt 1**	**Art. 57.** Prezes Urzędu w drodze decyzji: 1) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 rozporządzenia 2016/679;	
	4. Wykonywanie uprawnień powierzonych organowi nadzorczemu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom - w tym prawu do skutecznego środka ochrony prawnej przed sądem i rzetelnego procesu, określonym w prawie Unii i prawie państwa członkowskiego zgodnie z Kartą praw podstawowych. 5. Każde państwo członkowskie przewiduje w swoich przepisach, że jego organ nadzorczy jest uprawniony do wniesienia do organów wymiaru sprawiedliwości sprawy dotyczącej naruszenia niniejszego rozporządzenia oraz w stosownych przypadkach do wszczęcia lub do uczestniczenia w inny sposób w postępowaniu sądowym w celu wyegzekwowania stosowania przepisów niniejszego	**T** **T**	**Art. 98** **Art. 99**	**Art. 98**. 1. W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie w postępowaniu przed sądem, Prezes Urzędu może wytaczać powództwa na rzecz osoby, której dane dotyczą, za jej zgodą, a także wstępować, za zgodą powoda, do postępowania w każdym jego stadium. 2. W pozostałych sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych Prezes Urzędu może wstępować, za zgodą powoda, do	

	rozporządzenia.			postępowania przed sądem w każdym jego stadium, chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych. 3. W przypadkach, o których mowa w ust. 1 i 2, do Prezesa Urzędu stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 155, 398 i 416) o prokuratorze. **Art. 99**. Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, przedstawia sądowi istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych.	
	6. Każde państwo członkowskie może przewidzieć w swoich przepisach, że jego organowi nadzorczemu przysługują poza uprawnieniami określonymi w ust. 1, 2 i 3 także inne uprawnienia. Wykonywanie tych uprawnień nie może utrudniać skutecznego stosowania przepisów rozdziału VII.	**T**	**Art. 53**	**Art. 53**. 1. Prezes Urzędu może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. 2. Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. 3. Podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania	
Art. 59	**Sprawozdanie z działalności** Każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu naruszeń i rodzaje środków podjętych zgodnie z art. 58 ust. 2. Sprawozdania te są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem państwa członkowskiego. Są one udostępniane opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.	**T**	**Art. 51**	**Art. 51**. 1. Prezes Urzędu raz w roku do dnia 31 sierpnia przedstawia Sejmowi, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności, zawierające w szczególności informację o liczbie i rodzaju prawomocnych orzeczeń sądowych uwzględniających skargi na decyzje lub postanowienia Prezesa Urzędu oraz wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych. 2. Prezes Urzędu udostępnia sprawozdanie, o którym mowa ust. 1, na swojej stronie podmiotowej	

				Biuletynu Informacji Publicznej.	
ROZDZIAŁ VII **WSPÓŁPRACA I SPÓJNOŚĆ**					
Sekcja 1 **Współpraca**					
Art. 60	**Współpraca między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy** 1. Wiodący organ nadzorczy współpracuje z innymi organami nadzorczymi, których sprawa dotyczy, zgodnie z niniejszym artykułem w celu osiągnięcia porozumienia. Wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, wymieniają się wszelkimi stosownymi informacjami.	**N**			
	2. Wiodący organ nadzorczy może w dowolnym momencie zwrócić się do innych organów nadzorczych, których sprawa dotyczy, o wzajemną pomoc zgodnie z art. 61 i może prowadzić wspólne operacje zgodnie z art. 62, w szczególności w celu przeprowadzenia postępowania lub monitorowania wdrażania środka dotyczącego administratora lub podmiotu przetwarzającego posiadającego jednostkę organizacyjną w innym państwie członkowskim.	**N**			
	3. Wiodący organ nadzorczy niezwłocznie przekazuje innym organom nadzorczym, których sprawa dotyczy, stosowne informacje dotyczące danej sprawy. Niezwłocznie przedkłada innym organom, których sprawa dotyczy, nadzorczym projekt decyzji w celu uzyskania ich opinii i należytego uwzględnienia ich uwag.	**N**			
	4. Jeżeli w terminie czterech tygodni od otrzymania wniosku o opinię zgodnie z ust. 3 niniejszego artykułu inny organ nadzorczy, którego sprawa dotyczy, zgłosi mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji, wiodący organ nadzorczy - jeżeli nie przychyla się do mającego znaczenie dla sprawy i uzasadnionego sprzeciwu lub sądzi, że sprzeciw nie ma znaczenia dla sprawy lub nie jest uzasadniony -przekazuje sprawę w ramach mechanizmu spójności, o którym mowa w art. 63.	**N**			
	5. Jeżeli wiodący organ nadzorczy zamierza przychylić się do zgłoszonego mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, przedkłada innym organom nadzorczym, których sprawa dotyczy, zmieniony projekt decyzji w celu uzyskania ich opinii. Zmieniony projekt decyzji jest poddawany procedurze, o której mowa w ust. 4, w terminie dwóch tygodni.	**N**			
	6. Jeżeli w terminie, o którym mowa w ust. 4 i 5, żaden inny organ nadzorczy, którego sprawa dotyczy, nie zgłosi sprzeciwu wobec projektu decyzji przedłożonego przez wiodący organ nadzorczy, uznaje się, że wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, porozumiały się w sprawie projektu decyzji i są nią związane.	**N**			
	7. Wiodący organ nadzorczy przyjmuje decyzję i doręcza ją odpowiednio głównej lub pojedynczej jednostce organizacyjnej administratora lub podmiotu przetwarzającego oraz informuje o decyzji inne organy nadzorcze, których sprawa dotyczy, i Europejską Radę Ochrony Danych, dołączając streszczenie stanu	**N**			

	faktycznego i powodów decyzji. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o decyzji. 8. W drodze wyjątku od ust. 7, jeżeli skarga zostaje oddalona lub odrzucona, organ nadzorczy, do którego wniesiono skargę, przyjmuje decyzję i doręcza ją skarżącemu oraz informuje o niej administratora. 9. Jeżeli wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, porozumiały się co do oddalenia lub odrzucenia części skargi oraz co do podjęcia działań względem innych części tej skargi, dla każdej z tych części przyjmuje się odrębną decyzję. Wiodący organ nadzorczy przyjmuje decyzję w sprawie części dotyczącej działań względem administratora i doręcza ją głównej lub pojedynczej jednostce organizacyjnej administratora lub podmiotu przetwarzającego na terytorium swojego państwa członkowskiego i informuje o niej skarżącego, a organ nadzorczy skarżącego przyjmuje decyzję w sprawie części dotyczącej oddalenia lub odrzucenia tej skargi, doręcza ją skarżącemu oraz informuje o niej administratora lub podmiot przetwarzający. 10. Po doręczeniu administratorowi lub podmiotowi przetwarzającemu decyzji wiodącego organu nadzorczego zgodnie z ust. 7 i 9, podejmują oni niezbędne działania, by zastosować się do tej decyzji, jeżeli chodzi o czynności przetwarzania w ramach wszystkich swoich jednostek organizacyjnych w Unii. Administrator lub podmiot przetwarzający zawiadamiają wiodący organ nadzorczy o działaniach podjętych w celu zastosowania się do decyzji, ten zaś informuje o nich inne organy nadzorcze, których sprawa dotyczy. 11. Jeżeli w wyjątkowych okolicznościach organ nadzorczy, którego sprawa dotyczy, ma powody sądzić, że istnieje pilna potrzeba podjęcia działań w celu ochrony interesów osób, których dane dotyczą, zastosowanie ma tryb pilny, o którym mowa w art. 66. 12. Wiodący organ nadzorczy i inne organy nadzorcze, których sprawa dotyczy, dostarczają sobie nawzajem informacji wymaganych na mocy niniejszego artykułu drogą elektroniczną w standardowym formacie.	**N** **N** **N** **N** **N**			
Art. 61	**Wzajemna pomoc** 1. Organy nadzorcze przekazują sobie stosowne informacje i świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania niniejszego rozporządzenia oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o udzielenie uprzednich zezwoleń i przeprowadzenie uprzednich konsultacji oraz o przeprowadzenie kontroli i postępowań wyjaśniających. 2. Każdy organ nadzorczy podejmuje wszelkie odpowiednie środki, by odpowiedzi na wniosek innego organu nadzorczego udzielić bez zbędnej zwłoki i nie później niż w terminie miesiąca od otrzymania wniosku. Środki takie mogą obejmować w szczególności przekazanie stosownych informacji o przebiegu postępowania.	**N** **N**			

	3. Wniosek o pomoc zawiera wszelkie niezbędne informacje, w tym cel i uzasadnienie wniosku. Uzyskane informacje są wykorzystywane wyłącznie do celu, w którym o nie wystąpiono. 4. Wezwany organ nadzorczy nie może odmówić wykonania wniosku, chyba że: a) nie jest organem właściwym w przedmiocie wniosku lub środków, o których wykonanie wystąpiono; lub b) wykonanie wniosku stanowiłoby naruszenie niniejszego rozporządzenia, prawa Unii lub prawa państwa członkowskiego, któremu podlega wezwany organ nadzorczy. 5. Wezwany organ nadzorczy informuje wzywający organ nadzorczy, od którego wniosek pochodzi, o rezultatach lub w stosownym przypadku o postępach lub środkach zastosowanych w związku z tym wnioskiem. Wezwany organ nadzorczy uzasadnia odmowę wykonania wniosku na mocy ust. 4. 6. Wezwane organy nadzorcze przekazują informacje żądane przez inne organy nadzorcze zasadniczo drogą elektroniczną w standardowym formacie. 7. Wezwane organy nadzorcze nie pobierają opłat za działania podejmowane w związku z wnioskiem o wzajemną pomoc. Organy nadzorcze mogą uzgodnić zasady dokonywania wzajemnego zwrotu konkretnych wydatków poniesionych w wyniku świadczenia wzajemnej pomocy w wyjątkowych okolicznościach. 8. Jeżeli organ nadzorczy nie dostarczy informacji, o których mowa w ust. 5 niniejszego artykułu, w terminie miesiąca od otrzymania wniosku innego organu nadzorczego, wzywający organ nadzorczy może zastosować środek tymczasowy na terytorium swojego państwa członkowskiego zgodnie z art. 55 ust. 1. W takiej sytuacji uznaje się, że zgodnie z art. 66 ust. 1 zachodzi pilna potrzeba działania i że zgodnie z art. 66 ust. 2 wymagana jest pilna wiążąca decyzja Europejskiej Rady Ochrony Danych. 9. Komisja może w drodze aktów wykonawczych określić formułę i procedurę wzajemnej pomocy, o której mowa w niniejszym artykule, oraz zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności standardowy format, o którym mowa w ust. 6 niniejszego artykułu. Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.	**N** **N** **N** **N** **N** **T** **N**	**Art. 75**	**Art. 75.** 1. W przypadkach, o których mowa w art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 rozporządzenia 2016/679, Prezes Urzędu może wydać postanowienie o zastosowaniu środka tymczasowego, o którym mowa w art. 70 ust. 1. 2. W postanowieniu Prezes Urzędu określa termin obowiązywania środka tymczasowego, o którym mowa w art. 70 ust. 1, nie dłuższy niż 3 miesiące. 3. Na postanowienie przysługuje skarga do sądu administracyjnego.	
Art. 62	**Wspólne operacje organów nadzorczych** 1. Organy nadzorcze prowadzą w stosownych przypadkach wspólne operacje, w tym wspólne postępowania i wspólne działania egzekucyjne, w których uczestniczą członkowie lub personel organów nadzorczych innych państw członkowskich.	**T**	**Art. 77**	**Art. 77**. W przypadku otrzymania przez Prezesa Urzędu wniosku organu nadzorczego innego państwa członkowskiego Unii Europejskiej dotyczącego uczestnictwa we wspólnej operacji, o której mowa w art. 62 ust. 1 rozporządzenia 2016/679, albo wystąpienia przez Prezesa Urzędu z takim wnioskiem, Prezes Urzędu dokonuje z organem nadzorczym innego państwa członkowskiego Unii Europejskiej ustaleń	

				dotyczących wspólnej operacji i niezwłocznie sporządza wykaz ustaleń.	
	2. Jeżeli administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w kilku państwach członkowskich lub jeżeli operacje przetwarzania mogą istotnie wpłynąć na znaczną liczbę osób, których dane dotyczą, w więcej niż jednym państwie członkowskim, organ nadzorczy każdego z tych państw członkowskich ma prawo uczestniczyć we wspólnych operacjach. Organ nadzorczy, który jest właściwy zgodnie z art. 56 ust. 1 lub 4 zaprasza organ nadzorczy każdego z tych państw członkowskich do uczestnictwa w danych wspólnych operacjach i niezwłocznie odpowiada na wniosek organu nadzorczego dotyczący uczestnictwa.	**N**			
	3. Organ nadzorczy może zgodnie z prawem państwa członkowskiego i za zgodą organu nadzorczego oddelegowującego pracownika przyznać uprawnienia, w tym uprawnienia do prowadzenia postępowań wyjaśniających, członkom lub personelowi organu nadzorczego oddelegowującego pracownika uczestniczącym we wspólnych operacjach lub - jeżeli zezwala na to prawo państwa członkowskiego przyjmującego organu nadzorczego - zezwolić członkom lub personelowi organu nadzorczego oddelegowującego pracownika na wykonywanie ich własnych uprawnień w zakresie prowadzenia postępowań wyjaśniających zgodnie z prawem państwa członkowskiego organu nadzorczego oddelegowującego pracownika. Uprawnienia takie mogą być wykonywane wyłącznie pod kierownictwem i w obecności członków lub personelu przyjmującego organu nadzorczego. Członkowie lub personel organu nadzorczego oddelegowującego pracownika podlegają prawu państwa członkowskiego przyjmującego organu nadzorczego.	**T**	**Art. 79**	**Art. 79.**1. Kontrolę przeprowadza upoważniony przez Prezesa Urzędu: 1) pracownik Urzędu, 2) członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 rozporządzenia 2016/679 - zwany dalej „kontrolującym". 2. Kontrolujący o którym mowa w ust. 1 pkt 2, jest obowiązany do zachowania w tajemnicy informacji, o których dowiedział się w toku kontroli.	
	4. Jeżeli zgodnie z ust. 1 personel organu nadzorczego oddelegowującego pracownika działa w innym państwie członkowskim, państwo członkowskie przyjmującego organu nadzorczego ponosi odpowiedzialność za czynności tego personelu, w tym odpowiedzialność prawną za wszelkie szkody wyrządzone przez ten personel w trakcie operacji, zgodnie z prawem państwa członkowskiego, na którego terytorium ten personel działa.	**N**			
	5. Państwo członkowskie, na którego terytorium została wyrządzona szkoda, naprawia taką szkodę na warunkach mających zastosowanie do szkód wyrządzonych przez jego własny personel. Państwo członkowskie organu nadzorczego oddelegowującego pracownika, którego personel wyrządził szkodę wobec osoby na terytorium innego państwa członkowskiego, zwraca temu innemu państwu członkowskiemu całą kwotę, którą zapłaciło ono osobom uprawnionym w jego imieniu.	**N**			

	6. Bez uszczerbku dla możliwości dochodzenia swoich praw wobec osób trzecich i z wyjątkiem ust. 5, każde państwo członkowskie powstrzymuje się w przypadku określonym w ust. 1 od żądania odszkodowania od innego państwa członkowskiego za szkody, o których mowa w ust. 4. 7. Jeżeli planowana jest wspólna operacja, a organ nadzorczy nie wywiąże się w terminie miesiąca z obowiązku określonego w ust. 2 zdanie drugie niniejszego artykułu, pozostałe organy nadzorcze mogą przyjąć środek tymczasowy na terytorium swojego państwa członkowskiego zgodnie z art. 55. W takiej sytuacji uznaje się, że zgodnie z art. 66 ust. 1 zachodzi pilna potrzeba działania i że zgodnie z art. 66 ust. 2 wymagana jest pilna opinia lub pilna wiążąca decyzja Europejskiej Rady Ochrony Danych.	**N** **T**	**Art. 75** **Art. 70**	**Art. 75.** 1. W przypadkach, o których mowa w art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 rozporządzenia 2016/679, Prezes Urzędu może wydać postanowienie o zastosowaniu środka tymczasowego, o którym mowa w art. 70 ust. 1. 2. W postanowieniu Prezes Urzędu określa termin obowiązywania środka tymczasowego, o którym mowa w art. 70 ust. 1, nie dłuższy niż 3 miesiące. 3. Na postanowienie przysługuje skarga do sądu administracyjnego. **Art. 70. 1.** Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, Prezes Urzędu, w celu zapobieżenia tym skutkom, może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych wskazując dopuszczalny zakres tego przetwarzania. 2. W postanowieniu, o którym mowa w ust. 1, Prezes Urzędu określa termin obowiązywania ograniczenia przetwarzania danych osobowych nie dłuższy niż do dnia wydania decyzji kończącej postępowanie w sprawie. 3. Na postanowienie przysługuje skarga do sądu administracyjnego.	
Sekcja 2 **Spójność**					
Art. 63	**Mechanizm spójności** Aby przyczynić się do spójnego stosowania niniejszego rozporządzenia w całej Unii, organy nadzorcze współpracują ze sobą, a w stosownym przypadku także z Komisją, stosując mechanizm spójności określony w niniejszej sekcji.	**N**			
Art. 64	**Opinia Europejskiej Rady Ochrony Danych** 1. Europejska Rada Ochrony Danych wydaje opinię w przypadku, gdy	**N**			

	właściwy organ nadzorczy zamierza przyjąć środek wymieniony poniżej. W tym celu właściwy organ nadzorczy zgłasza Europejskiej Radzie Ochrony Danych projekt decyzji dotyczącej: a) przyjęcia na mocy art. 35 ust. 4 wykazu operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych; b) stwierdzenia zgodnie z art. 40 ust. 7, czy projekt kodeksu postępowania, zmiana kodeksu lub rozszerzenie jego zakresu są zgodne z niniejszym rozporządzeniem; c) zatwierdzenia kryteriów akredytacji podmiotu na mocy art. 41 ust. 3 lub podmiotu certyfikującego na mocy art. 43 ust. 3; d) określenia standardowych klauzul ochrony danych, o których mowa w art. 46 ust. 2 lit. d) i art. 28 ust. 8; e) wydania zezwolenia na klauzule umowne, o których mowa w art. 46 ust. 3; lub f) zatwierdzenia wiążących reguł korporacyjnych w rozumieniu art. 47. 2. Każdy organ nadzorczy, przewodniczący Europejskiej Rady Ochrony Danych lub Komisja mogą wystąpić o przeanalizowanie przez Europejską Radę Ochrony Danych w celu wydania opinii sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim, w szczególności jeżeli właściwy organ nadzorczy nie wywiązuje się z obowiązków dotyczących wzajemnej pomocy zgodnie z art. 61 lub wspólnych operacji zgodnie z art. 62. 3. W przypadkach, o których mowa w ust. 1 i 2, Europejska Rada Ochrony Danych wydaje opinię w przedłożonej jej sprawie, o ile wcześniej nie wydała już opinii w takiej samej sprawie. Europejska Rady Ochrony Danych przyjmuje tę opinię w terminie ośmiu tygodni zwykłą większością głosów swoich członków. Ze względu na złożony charakter sprawy termin ten można przedłużyć o sześć tygodni. Jeżeli chodzi o projekt decyzji, o którym mowa w ust. 1 i który został przekazany członkom Europejskiej Rady Ochrony Danych zgodnie z ust. 5, uznaje się, że członek, który w rozsądnym terminie wskazanym przez przewodniczącego nie zgłosił sprzeciwu, zgadza się z tym projektem. 4. Organy nadzorcze i Komisja przekazują bez zbędnej zwłoki Europejskiej Radzie Ochrony Danych drogą elektroniczną w standardowym formacie wszelkie stosowne informacje, w tym w odpowiednim przypadku streszczenie stanu faktycznego, projekt decyzji, powody przemawiające za koniecznością przyjęcia takiego środka oraz opinię innych organów nadzorczych, których sprawa dotyczy. 5. Przewodniczący Europejskiej Rady Ochrony Danych bez zbędnej zwłoki przekazuje drogą elektroniczną: a) członkom Europejskiej Rady Ochrony Danych i Komisji wszelkie stosowne informacje otrzymane w standardowym formacie. W razie potrzeby sekretariat Europejskiej Rady Ochrony Danych zapewnia tłumaczenie stosownych informacji; oraz b) organowi nadzorczemu, o którym zależnie od sytuacji mowa w ust. 1 i 2, oraz Komisji opinię, którą podaje też do wiadomości publicznej. 6. Właściwy organ nadzorczy nie przyjmuje projektu decyzji, o którym mowa w art. ust. 1 przed upływem terminu, o którym mowa w ust. 3. 7. Organ nadzorczy, o którym mowa w ust. 1, w jak największym stopniu uwzględnia opinię Europejskiej Rady Ochrony Danych i w terminie dwóch tygodni po otrzymaniu tej opinii informuje drogą elektroniczną przewodniczącego Europejskiej Rady Ochrony Danych, czy podtrzymuje projekt decyzji, czy też go zmieni, a w stosownym przypadku przekazuje mu w standardowym formacie zmieniony projekt decyzji.				

	8. Jeżeli w terminie, o którym mowa w ust. 7 niniejszego artykułu, organ nadzorczy, którego sprawa dotyczy, poinformuje przewodniczącego Europejskiej Rady Ochrony Danych, że nie zamierza się zastosować do całości lub części jej opinii podając odpowiednie uzasadnienie, zastosowanie ma art. 65 ust. 1.				
Art. 65	**Rozstrzyganie sporów przez Europejską Radę Ochrony Danych** 1. Aby w poszczególnych sytuacjach zapewnić właściwe i spójne stosowanie niniejszego rozporządzenia, Europejska Rada Ochrony Danych przyjmuje w następujących przypadkach wiążące decyzje: a) jeżeli w przypadku, o którym mowa w art. 60 ust. 4, organ nadzorczy, którego sprawa dotyczy, zgłosił mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji wiodącego organu nadzorczego, a wiodący organ nadzorczy odrzucił taki sprzeciw jako niemający znaczenia dla sprawy lub nieuzasadniony. Wiążąca decyzja dotyczy wszystkich spraw, które są przedmiotem mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, w szczególności dotyczy tego, czy doszło do naruszenia niniejszego rozporządzenia; b) jeżeli panują sprzeczne opinie co do tego, który z organów nadzorczych, których sprawa dotyczy, jest właściwy względem głównej jednostki organizacyjnej; c) jeżeli właściwy organ nadzorczy nie wystąpił o opinię do Europejskiej Rady Ochrony Danych w przypadkach, o których mowa w art. 64 ust. 1, lub nie zastosował się do opinii Europejskiej Rady Ochrony Danych wydanej zgodnie z art. 64. W takim przypadku organ nadzorczy, którego sprawa dotyczy, lub Komisja mogą zgłosić sprawę Europejskiej Radzie Ochrony Danych. 2. Decyzję, o której mowa w ust. 1, Europejska Rada Ochrony Danych przyjmuje większością dwóch trzecich głosów swoich członków w terminie miesiąca od wpłynięcia sprawy. Ze względu na złożony charakter sprawy termin ten można przedłużyć o miesiąc. Decyzja, o której mowa w ust. 1, zostaje wraz z uzasadnieniem skierowana do wiodącego organu nadzorczego i wszystkich organów nadzorczych, których sprawa dotyczy, i jest dla nich wiążąca. 3. Jeżeli Europejska Rada Ochrony Danych nie jest w stanie przyjąć decyzji w terminach, o których mowa w ust. 2, przyjmuje decyzję w terminie dwóch tygodni po upłynięciu drugiego miesiąca, o którym mowa w ust. 2, zwykłą większością głosów swoich członków. Jeżeli głosy członków Europejskiej Rady Ochrony Danych rozkładają się po równo, decyduje głos przewodniczącego. 4. Przed upływem terminów, o których mowa w ust. 2 i 3, organy nadzorcze, których sprawa dotyczy, nie przyjmują decyzji w sprawie przedłożonej Europejskiej Radzie Ochrony Danych na mocy ust. 1. 5. Przewodniczący Europejskiej Rady Ochrony Danych bez zbędnej zwłoki notyfikuje organom nadzorczym, których sprawa dotyczy, decyzję, o której mowa w ust. 1. Informuje o niej Komisję. Decyzja jest niezwłocznie publikowana na stronie internetowej Europejskiej Rady Ochrony Danych, po tym jak organ nadzorczy notyfikował ostateczną decyzję, o której mowa w ust. 6. 6. Bez zbędnej zwłoki i najpóźniej w terminie miesiąca po notyfikowaniu przez Europejską Radę Ochrony Danych swojej decyzji, wiodący organ nadzorczy lub w stosownym przypadku organ nadzorczy, do którego wniesiono skargę, przyjmuje ostateczną decyzję na podstawie decyzji, o której mowa w ust. 1 niniejszego artykułu. Wiodący organ nadzorczy lub w stosownym przypadku organ	**N**			

	nadzorczy, do którego wniesiono skargę, informuje Europejską Radę Ochrony Danych o terminie, w którym doręczono ostateczną decyzję odpowiednio administratorowi lub podmiotowi przetwarzającemu oraz osobie, której dane dotyczą. Ostateczna decyzja organów nadzorczych, których sprawa dotyczy, zostaje przyjęta w trybie art. 60 ust. 7, 8 i 9. Ostateczna decyzja zawiera informacje o decyzji, o której mowa w ust. 1 niniejszego artykułu, i wskazuje, że decyzja, o której mowa w tym ustępie, zostanie opublikowana na stronie internetowej Europejskiej Rady Ochrony Danych zgodnie z ust. 5 niniejszego artykułu. Do ostatecznej decyzji załączona zostaje decyzja, o której mowa w ust. 1 niniejszego artykułu.				
Art. 66	**Tryb pilny** 1. W wyjątkowych okolicznościach, jeżeli organ nadzorczy, którego sprawa dotyczy, uzna, że istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, może w drodze odstępstwa od mechanizmu spójności, o którym mowa w art. 63, 64 i 65, lub od procedury, o której mowa w art. 60, niezwłocznie przyjąć środki tymczasowe mające na terytorium jego państwa członkowskiego wywołać skutki prawne przez określony okres, nieprzekraczający trzech miesięcy. Organ nadzorczy niezwłocznie informuje o tych środkach i o powodach ich przyjęcia pozostałe organy nadzorcze, których sprawa dotyczy, Europejską Radę Ochrony Danych i Komisję. 2. Jeżeli organ nadzorczy zastosował środek na mocy ust. 1 i uznaje, że należy pilnie przyjąć środki o charakterze ostatecznym, może zwrócić się z wnioskiem o pilne wydanie opinii lub wiążącej decyzji do Europejskiej Rady Ochrony Danych, uzasadniając swój wniosek o taką opinię lub decyzję. 3. Organ nadzorczy może zwrócić się do Europejskiej Rady Ochrony Danych z wnioskiem o pilne wydanie opinii lub w stosownym przypadku wiążącej decyzji, uzasadniając swój wniosek o taką opinię lub decyzję, w tym uzasadniając pilną potrzebę działań - jeżeli właściwy organ nadzorczy nie zastosował odpowiedniego środka w sytuacji, w której istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą. 4. W drodze wyjątku od art. 64 ust. 3 i art. 65 ust. 2, Europejska Rada Ochrony Danych przyjmuje opinię lub wiążącą decyzję wydawane w trybie pilnym, o których mowa w ust. 2 i 3 niniejszego artykułu, w terminie dwóch tygodni zwykłą większością głosów swoich członków.	**T**	**Art. 75** **Art. 70**	**Art. 75.** 1. W przypadkach, o których mowa w art. 61 ust. 8, art. 62 ust. 7 i art. 66 ust. 1 rozporządzenia 2016/679, Prezes Urzędu może wydać postanowienie o zastosowaniu środka tymczasowego, o którym mowa w art. 70 ust. 1. 2. W postanowieniu Prezes Urzędu określa termin obowiązywania środka tymczasowego, o którym mowa w art. 70 ust. 1, nie dłuższy niż 3 miesiące. 3. Na postanowienie przysługuje skarga do sądu administracyjnego. **Art. 70. 1.** Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, Prezes Urzędu, w celu zapobieżenia tym skutkom, może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych wskazując dopuszczalny zakres tego przetwarzania. 2. W postanowieniu, o którym mowa w ust. 1, Prezes Urzędu określa termin obowiązywania ograniczenia przetwarzania danych osobowych nie dłuższy niż do dnia wydania decyzji kończącej postępowanie w sprawie. 3. Na postanowienie przysługuje skarga do sądu administracyjnego.	
Art. 67	**Wymiana informacji** Komisja może przyjmować akty wykonawcze o charakterze ogólnym, w celu określenia zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności standardowy format, o którym mowa w art. 64. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.	**N**			

Sekcja 3 **Europejska Rada Ochrony Danych**					
Art. 68	**Europejska Rada Ochrony Danych** 1. Niniejszym ustanawia się Europejską Radę Ochrony Danych jako organ Unii posiadający osobowość prawną. 2. Europejską Radę Ochrony Danych reprezentuje jej przewodniczący. 3. Do Europejskiej Rady Ochrony Danych należą: przewodniczący jednego organu nadzorczego każdego państwa członkowskiego oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele. 4. Jeżeli w państwie członkowskim za monitorowanie stosowania przepisów na mocy niniejszego rozporządzenia odpowiada więcej niż jeden organ nadzorczy, to zgodnie z prawem tego państwa członkowskiego wyznaczony zostaje wspólny przedstawiciel. 5. Komisja ma prawo do udziału w działaniach i posiedzeniach Europejskiej Rady Ochrony Danych, nie ma jednak prawa głosowania. Komisja wyznacza swojego przedstawiciela. Przewodniczący Europejskiej Rady Ochrony Danych informuje Komisję o działaniach Europejskiej Rady Ochrony Danych. 6. W kwestiach, o których mowa w art. 65, Europejski Inspektor Ochrony Danych ma prawo głosowania wyłącznie względem decyzji co do zasad i przepisów, które mają zastosowanie do instytucji, organów i jednostek organizacyjnych Unii i merytorycznie odpowiadają przepisom niniejszego rozporządzenia.	**N**			
Art. 69	**Niezależność** 1. W toku wypełniania swoich zadań lub wykonywania swoich uprawnień na mocy art. 70 i 71 Europejska Rada Ochrony Danych działa w sposób niezależny. 2. Bez uszczerbku dla wniosków Komisji, o których mowa w art. 70 ust. 1 lit. b) i art. 70 ust. 2, Europejska Rada Ochrony Danych podczas wypełniania swoich zadań lub wykonywania swoich uprawnień nie zwraca się do nikogo o instrukcje ani ich od nikogo nie przyjmuje.	**N**			
Art. 70	**Zadania Europejskiej Rady Ochrony Danych** 1. Europejska Rada Ochrony Danych zapewnia spójne stosowanie niniejszego rozporządzenia. W tym celu z własnej inicjatywy lub w stosownych przypadkach na wniosek Komisji podejmuje w szczególności następujące działania: a) monitoruje i zapewnia właściwe stosowanie niniejszego rozporządzenia w przypadkach, o których mowa w art. 64 i 65, bez uszczerbku dla zadań krajowych organów nadzorczych; b) doradza Komisji w sprawach związanych z ochroną danych osobowych w Unii, w tym w sprawie wszelkich proponowanych zmian do niniejszego rozporządzenia; c) doradza Komisji w sprawie formatu i procedur wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi	**N**			

		do celów wiążących reguł korporacyjnych;				
	d)	wydaje wytyczne, zalecenia oraz określa najlepsze praktyki dotyczące usuwania z ogólnodostępnych usług łączności łącz do danych osobowych, kopi tych danych lub ich replikacji, o czym mowa w art. 17 ust. 2;				
	e)	z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji bada wszelkie kwestie dotyczące stosowania niniejszego rozporządzenia i wydaje wytyczne, zalecenia oraz określa najlepsze praktyki, by zachęcić do spójnego stosowania niniejszego rozporządzenia;				
	f)	wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by na potrzeby art. 22 ust. 2 doprecyzować kryteria i wymogi dotyczące decyzji opartych na profilowaniu;				
	g)	wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu dotyczące stwierdzania naruszenia ochrony danych osobowych i określenia zbędnej zwłoki w rozumieniu art. 33 ust. 1 i 2 oraz szczególnych okoliczności, w których administrator lub podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych;				
	h)	wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu wskazujące, w jakich okolicznościach naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych w rozumieniu art. 34 ust. 1;				
	i)	wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by doprecyzować kryteria i wymogi względem przekazywania danych osobowych, które opiera się na wiążących regułach korporacyjnych stosowanych przez administratorów i na wiążących regułach korporacyjnych stosowanych przez podmioty przetwarzające, oraz inne konieczne wymogi mające zapewnić ochronę danych osobowych osób, których dane dotyczą, zgodnie z art. 47;				
	j)	wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by doprecyzować kryteria i wymogi względem przekazywania danych osobowych na podstawie art. 49 ust. 1;				
	k)	opracowuje wytyczne dla organów nadzorczych w sprawie stosowania środków, o których mowa w art. 58 ust. 1, 2 i 3, oraz w sprawie określania wysokości administracyjnych kar pieniężnych zgodnie z art. 83;				
	l)	dokonuje przeglądu praktycznego stosowania wytycznych, zaleceń i najlepszych praktyk, o których mowa w lit. e) i f);				
	m)	wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by na potrzeby art. 54 ust. 2 określić wspólne procedury postępowania w przypadkach zgłaszania przez osoby fizyczne naruszeń niniejszego rozporządzenia;				
	n)	zachęca do sporządzania kodeksów postępowania oraz do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń w tej dziedzinie zgodnie z art. 40 i 42;				
	o)	akredytuje podmioty certyfikujące i dokonuje okresowego przeglądu certyfikacji zgodnie z art. 43 oraz prowadzi publiczny rejestr podmiotów akredytowanych zgodnie z art. 43 ust. 6 i administratorów i podmiotów przetwarzających akredytowanych zgodnie z art. 42 ust. 7, mających siedzibę w państwach trzecich;				
	p)	precyzuje wymogi, o których mowa w art. 43 ust. 3, z myślą o akredytacji podmiotów certyfikujących zgodnie z art. 42;				
	q)	udziela Komisji opinii w sprawie wymogów certyfikacyjnych, o których				

	mowa w art. 43 ust. 8; r) udziela Komisji opinii w sprawie znaków graficznych, o których mowa w art. 12 ust. 7; s) udziela Komisji opinii na potrzeby oceny, czy stopień ochrony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni, w tym na potrzeby oceny, czy państwo trzecie, terytorium, określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa nie przestały zapewniać odpowiedniego stopnia ochrony. W tym celu Komisja udostępnia Europejskiej Radzie Ochrony Danych wszelką niezbędną dokumentację, w tym korespondencję z rządem państwa trzeciego w odniesieniu do tego państwa trzeciego, terytorium lub określonego sektora lub korespondencję z organizacją międzynarodową; t) wydaje opinie w sprawie projektów decyzji zgłoszonych przez organy nadzorcze zgodnie z mechanizmem spójności, o którym mowa w art. 64 ust. 1, w sprawach przedłożonych jej zgodnie z art. 64 ust. 2 oraz wydaje wiążące decyzje zgodnie z art. 65, w tym w sprawach, o których mowa w art. 66; u) upowszechnia współpracę oraz skuteczną dwustronną i wielostronną wymianę informacji i dobrych praktyk między organami nadzorczymi; v) upowszechnia wspólne programy szkoleń oraz ułatwia wymianę personelu między organami nadzorczymi, a w stosownych przypadkach - z organami nadzorczymi państw trzecich lub organizacji międzynarodowych; w) upowszechnia wymianę wiedzy i dokumentów na temat ustawodawstwa i praktyki w dziedzinie ochrony danych z organami nadzorczymi odpowiedzialnymi za ochronę danych na świecie; x) wydaje opinie na temat kodeksów postępowania opracowywanych na szczeblu Unii zgodnie z art. 40 ust. 9; oraz y) prowadzi publicznie dostępny elektroniczny rejestr decyzji podjętych przez organy nadzorcze i wyroków sądowych w sprawach rozpatrywanych w ramach mechanizmu spójności. 2. Jeżeli Komisja zwraca się do Europejskiej Rady Ochrony Danych o konsultację, może zależnie od pilności sprawy wskazać termin udzielenia odpowiedzi. 3. Europejska Rada Ochrony Danych przekazuje swoje opinie, wytyczne, zalecenia i najlepsze praktyki Komisji i komitetowi, o którym mowa w art. 93, oraz podaje je do wiadomości publicznej. 4. Europejska Rada Ochrony Danych konsultuje się w stosownych przypadkach ze stronami, których sprawa dotyczy, i daje im możliwość przestawienia uwag w rozsądnym terminie. Bez uszczerbku dla art. 76 Europejska Rada Ochrony Danych podaje wyniki procedury konsultacji do wiadomości publicznej.				
Art. 71	**Sprawozdania** 1. Europejska Rada Ochrony Danych sporządza roczne sprawozdanie na temat ochrony osób fizycznych w związku z przetwarzaniem danych w Unii, a w stosownym przypadku w państwach trzecich i organizacjach międzynarodowych. Sprawozdanie zostaje podane do wiadomości publicznej oraz przekazane Parlamentowi Europejskiemu, Radzie i Komisji. 2. Sprawozdanie roczne obejmuje przegląd praktycznego stosowania wytycznych, zaleceń i najlepszych praktyk, o których mowa w art. 70 ust. 1 lit. l),	**N**			

	oraz wiążących decyzji, o których mowa w art. 65.				
Art. 72	**Procedura** 1. Europejska Rada Ochrony Danych podejmuje decyzje zwykłą większością głosów swoich członków, o ile niniejsze rozporządzenie nie przewiduje inaczej. 2. Europejska Rada Ochrony Danych przyjmuje swój regulamin wewnętrzny większością dwóch trzecich głosów swoich członków i określa swoje zasady działania.	**N**			
Art. 73	**Przewodniczący** 1. Europejska Rada Ochrony Danych wybiera zwykłą większością głosów spośród swoich członków przewodniczącego i dwóch wiceprzewodniczących. 2. Kadencja przewodniczącego i wiceprzewodniczących trwa pięć lat i może zostać jednokrotnie powtórzona.	**N**			
Art. 74	**Zadania przewodniczącego** 1. Przewodniczący ma następujące zadania: a) zwołuje posiedzenia Europejskiej Rady Ochrony Danych i sporządza porządek obrad; b) notyfikuje wiodącemu organowi nadzorczemu i organom nadzorczym, których sprawa dotyczy, decyzje przyjęte przez Europejską Radę Ochrony Danych na mocy art. 65; c) zapewnia terminowe wykonanie zadań Europejskiej Rady Ochrony Danych, w szczególności w odniesieniu do mechanizmu spójności, o którym mowa w art. 63. 2. Europejska Rada Ochrony Danych określa w swoim regulaminie wewnętrznym podział zadań między przewodniczącego a wiceprzewodniczących.	**N**			
Art. 75	**Sekretariat** 1. Europejski Inspektor Ochrony Danych zapewnia obsługę sekretariatu dla Europejskiej Rady Ochrony Danych. 2. Sekretariat wykonuje swoje zadania wyłącznie pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych. 3. Personel Europejskiego Inspektora Ochrony Danych wykonujący zadania, które niniejsze rozporządzenie powierza Europejskiej Radzie Ochrony Danych, podlega oddzielnej hierarchii służbowej, innej niż personel wykonujący zadania powierzone Europejskiemu Inspektorowi Ochrony Danych. 4. W stosownych przypadkach Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych opracowują i publikują protokół ustaleń, który służy wykonaniu niniejszego artykułu: określa on warunki współpracy i ma zastosowanie do personelu Europejskiego Inspektora Ochrony Danych wykonującego zadania powierzone niniejszym rozporządzeniem Europejskiej Radzie Ochrony Danych. 5. Sekretariat zapewnia Europejskiej Radzie Ochrony Danych wsparcie analityczne, administracyjne i logistyczne.	**N**			

	6. Sekretariat odpowiada w szczególności za: a) bieżącą działalność Europejskiej Rady Ochrony Danych; b) komunikację między członkami Europejskiej Rady Ochrony Danych, jej przewodniczącym i Komisją; c) komunikację z innymi instytucjami i opinią publiczną; d) stosowanie elektronicznych środków komunikacji wewnętrznej i zewnętrznej; e) tłumaczenie stosownych informacji; f) przygotowywanie posiedzeń Europejskiej Rady Ochrony Danych oraz działania następcze w związku z nimi; g) przygotowywanie, redagowanie i publikowanie opinii, decyzji w sprawie rozstrzygnięcia sporów między organami nadzorczymi oraz innych tekstów przyjmowanych przez Europejską Radę Ochrony Danych.				
Art. 76	**Poufność** 1. Dyskusje Europejskiej Rady Ochrony Danych są poufne, jeżeli taką konieczność stwierdzi Rada zgodnie ze swoim regulaminem wewnętrznym. 2. Dostęp do dokumentów przedłożonych członkom Europejskiej Rady Ochrony Danych, ekspertom i przedstawicielom stron trzecich jest regulowany rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1049/2001.	**N**			
ROZDZIAŁ VIII ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE					
Art. 77	**Prawo do wniesienia skargi do organu nadzorczego** 1. Bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie. 2. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78.	**N** **T**	**Art. 62**	**Art. 62**. W przypadku, o którym mowa w art. 36 ustawy z dnia 14 czerwca 1960 r.− Kodeks postępowania administracyjnego, Prezes Urzędu zawiadamiając strony o niezałatwieniu sprawy w terminie, obowiązany jest również poinformować o stanie sprawy i przeprowadzonych w jej toku czynnościach.	
Art. 78	**Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu** 1. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej.	**N**			

	2. 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 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. 3. Postępowanie przeciwko organowi nadzorczemu zostaje wszczęte przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę. 4. Jeżeli postępowanie zostało wszczęte przeciwko decyzji organu nadzorczego, którą poprzedziła opinia lub decyzja Europejskiej Rady Ochrony Danych w ramach mechanizmu spójności, organ nadzorczy przekazuje sądowi tę opinię lub decyzję.	**N** **N**			
Art. 79	**Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu** 1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. *77,* każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia. 2. Postępowanie przeciwko administratorowi lub podmiotowi przetwarzającemu wszczyna się przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Ewentualnie postępowanie takie może zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.	**T**	**Art. 92 - 94**	**Art. 92**. W zakresie nieuregulowanym rozporządzeniem 2016/679 do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny. **Art. 93**. W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i 82 rozporządzenia 2016/679, jest właściwy sąd okręgowy. **Art. 94.** 1. O wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o którym mowa w art. 79 lub art. 82 rozporządzenia 2016/679, sąd zawiadamia niezwłocznie Prezesa Urzędu. 2. Prezes Urzędu zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona. Prezes Urzędu niezwłocznie informuje również sąd o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia.	
Art. 80	**Reprezentowanie osób, których dane dotyczą** 1. Osoba, której dane dotyczą, ma prawo umocować podmiot, organizację lub zrzeszenie - które nie mają charakteru zarobkowego, zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają cele statutowe leżące w interesie publicznym i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych - do wniesienia w jej imieniu skargi oraz wykonywania w jej imieniu praw, o których mowa w art. 77, 78 i 79, oraz żądania w jej imieniu odszkodowania, o którym mowa w art. 82, jeżeli przewiduje to prawo państwa członkowskiego. 2. Państwa członkowskie mogą przewidzieć, że podmiot, organizacja lub	**N** **T**	**Art. 61**	**Art. 61.** Organizacja społeczna, o której mowa w art. 31	

	zrzeszenie, o których mowa w ust. 1 niniejszego artykułu, mają - niezależnie od upoważnienia otrzymanego od osoby, której dane dotyczą - prawo wnieść w tym państwie członkowskim skargę do organu nadzorczego właściwego zgodnie z art. 77 oraz wykonać prawa, o których mowa w art. 78 i 79, jeżeli uznają, że w wyniku przetwarzania naruszone zostały prawa osoby, której dane dotyczą, wynikające z niniejszego rozporządzenia.			§ 1 ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego, może również występować w postępowaniu za zgodą osoby, której dane dotyczą w jej imieniu i na jej rzecz.	
Art. 81	**Zawieszenie postępowania** 1. Jeżeli właściwy sąd państwa członkowskiego posiada informację, że przed sądem w innym państwie członkowskim toczy się postępowanie w tej samej sprawie w odniesieniu do przetwarzania przez tego samego administratora lub ten sam podmiot przetwarzający, kontaktuje się z tym sądem w innym państwie członkowskim, aby potwierdzić istnienie takiego postępowania. 2. Jeżeli przed sądem w innym państwie członkowskim toczy się postępowanie w tej samej sprawie w odniesieniu do przetwarzania przez tego samego administratora lub ten sam podmiot przetwarzający, właściwy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić swoje postępowanie. 3. Jeżeli postępowania te toczą się w pierwszej instancji, sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może także - na wniosek jednej ze stron - stwierdzić brak swojej jurysdykcji, jeżeli sąd, przed którym jako pierwszym wszczęto postępowanie, ma jurysdykcję względem przedmiotowych spraw, a jego prawo dopuszcza ich połączenie.	**N**			
Art. 82	**Prawo do odszkodowania i odpowiedzialność** 1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. 2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. 3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. 4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. 5. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części	**N**			

	szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2. 6. Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2.				
Art. 83	**Ogólne warunki nakładania administracyjnych kar pieniężnych** 1. Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające. 2. Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)-h) oraz j). Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na: a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody; b) umyślny lub nieumyślny charakter naruszenia; c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą; d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32; e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego; f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków; g) kategorie danych osobowych, których dotyczyło naruszenie; h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie; i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 - przestrzeganie tych środków; j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty. 3. Jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie. 4. Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z	**N** **N** **N** **N** **N**			

	ust. 2 administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa: a) obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 -39 oraz 42 i 43; b) obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43; c) obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4; 5. Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa: a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9; b) praw osób, których dane dotyczą, o których mowa w art. 12-22; c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44-49; d) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX; e) nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1. 6. Nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 podlega na mocy ust. 2 niniejszego artykułu administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. 7. Bez uszczerbku dla uprawnień naprawczych organu nadzorczego, o których mowa w ust. 58 ust. 2, 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.	**N** **N** **T**	**Art. 101** **Art. 102**	**Art. 101**. Prezes Urzędu może nałożyć na podmiot, obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż: 1) jednostka sektora finansów publicznych w rozumieniu w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, 2) instytut badawczy w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, 3) Narodowy Bank Polski - w drodze decyzji, administracyjne kary pieniężne na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679. **Art. 102**. 1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na: 1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1 – 12 i 14 ustawy z	

				dnia 27 sierpnia 2009 r. o finansach publicznych 2) instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych; 3) Narodowy Bank Polski. 2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. 3. Administracyjne kary pieniężne, o których mowa w ust. 1 i 2, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.	
	8. Wykonywanie przez organ nadzorczy uprawnień powierzonych mu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom proceduralnym zgodnie z prawem Unii i prawem państwa członkowskiego, obejmującym prawo do skutecznego sądowego środka ochrony prawnej i rzetelnego procesu. 9. Jeżeli ustrój prawny państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, niniejszy artykuł można stosować w ten sposób, że o zastosowanie kary pieniężnej wnosi właściwy organ nadzorczy, a nakłada ją właściwy sąd krajowy, o ile zapewniona zostaje skuteczność tych rozwiązań prawnych i równoważność ich skutku względem administracyjnej kary pieniężnej nakładanej przez organ nadzorczy. Nakładane kary pieniężne muszą być w każdym przypadku skuteczne, proporcjonalne i odstraszające. W terminie określonym w art. 91 ust. 2 takie państwa członkowskie zawiadamiają Komisję o przepisach swojego prawa, które przyjęły zgodnie z niniejszym ustępem do dnia 25 maja 2018 r., a następnie niezwłocznie o wszelkich późniejszych aktach zmieniających lub zmianach mających wpływ na te przepisy.	**N** **N**			
Art. 84	**Sankcje** 1. Państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.	**T**	**Art. 73**	**Art. 73**. 1. Prezes Urzędu jeżeli uzna, że przemawia za tym interes publiczny, po zakończeniu postępowania, informuje o wydaniu decyzji na swojej stronie podmiotowej Biuletynu Informacji Publicznej. 2. Organy lub podmioty publiczne, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych oraz Narodowy Bank Polski, w stosunku do których Prezes Urzędu wydał prawomocną decyzję stwierdzającą naruszenie, niezwłocznie podają do publicznej wiadomości na swojej stronie internetowej lub stronie podmiotowej Biuletynu Informacji Publicznej, informację o działaniach podjętych w celu wykonania decyzji.	

	2. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych zgodnie z ust. 1, a następnie niezwłocznie o każdej późniejszej ich zmianie.	**N**			
ROZDZIAŁ IX **PRZEPISY DOTYCZĄCE SZCZEGÓLNYCH SYTUACJI ZWIĄZANYCH Z PRZETWARZANIEM**					
Art. 85	**Przetwarzanie a wolność wypowiedzi i informacji** 1. Państwa członkowskie przyjmują przepisy pozwalające pogodzić prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z wolnością wypowiedzi i informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej. 2. 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.	**T**	**Art. 2**	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.1)), a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5 – 9, art. 11, art. 13 - 16, art. 18 - 22, art. 27, art. 28 ust. 2 – 10 oraz art. 30 rozporządzenia 2016/679. 2. Do wypowiedzi akademickiej, o której mowa w art. 85 ust. 2 rozporządzenia 2016/679, nie stosuje się przepisów art. 13, art. 15 ust. 3 i 4, art. 18, art. 27, art. 28 ust. 2 – 10 oraz art. 30 rozporządzenia 2016/679.	
	3. Każde państwo członkowskie zawiadamia Komisję o przepisach, które przyjęło	**N**			

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

	zgodnie z ust. 2, a następnie niezwłocznie o wszelkich późniejszych aktach zmieniających lub zmianach ich dotyczących.				
Art. 86	**Przetwarzanie a publiczny dostęp do dokumentów urzędowych** Dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia.	**N**			
Art. 87	**Przetwarzanie krajowego numeru identyfikacyjnego** Państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie.	**N**			
Art. 88	**Przetwarzanie w kontekście zatrudnienia** 1. Państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy. 2. Przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.	**N**			

	3. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych na mocy ust. 1, a następnie niezwłocznie o każdej dotyczącej ich późniejszej zmianie.				
Art. 89	**Zabezpieczenia i wyjątki mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych** 1. Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikować osoby, której dane dotyczą, cele należy realizować w ten sposób. 2. W przypadku przetwarzania danych osobowych do celów badań naukowych lub historycznych lub do celów statystycznych prawo Unii lub prawo państwa członkowskiego mogą przewidzieć wyjątki od praw, o których mowa w art. 15, 16, 18 i 21, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 1 niniejszego artykułu, jeżeli jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację wspomnianych konkretnych celów, i jeżeli wyjątki takie są konieczne do realizacji tych celów. 3. W przypadku przetwarzania danych osobowych do celów archiwalnych w interesie publicznym prawo Unii lub prawo państwa członkowskiego mogą przewidzieć wyjątki od praw, o których mowa w art. 15, 16, 18, 19, 20 i 21, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 1 niniejszego artykułu, jeżeli jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację wspomnianych konkretnych celów, i jeżeli wyjątki takie są konieczne do realizacji tych celów. 4. Jeżeli przetwarzanie, o którym mowa w ust. 2 i 3, służy równocześnie innemu celowi, wspomniane wyjątki mają zastosowanie wyłącznie do przetwarzania w celach, o których mowa w tych ustępach.	**N**			

Art. 90	**Obowiązek zachowania tajemnicy** 1. Państwa członkowskie mogą przyjąć przepisy szczególne określające uprawnienia organów nadzorczych ustanowione w art. 58 ust. 1 lit. e) i f) wobec administratorów lub podmiotów przetwarzających, którzy podlegają - na mocy prawa Unii lub prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe - obowiązkowi zachowania tajemnicy zawodowej lub innym równoważnym obowiązkom zachowania tajemnicy, jeżeli jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy. Przepisy te mają zastosowanie wyłącznie do danych osobowych, które administrator lub podmiot przetwarzający otrzymali lub pozyskali w wyniku lub w ramach działania objętego tym obowiązkiem zachowania tajemnicy. 2. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach uchwalonych na mocy ust. 1, a następnie niezwłocznie o każdej dotyczącej ich późniejszej zmianie.	**T** **N**	**Art. 64**	**Art. 64**. W celu realizacji swoich zadań Prezes Urzędu ma prawo dostępu do informacji objętych tajemnicą prawnie chronioną, chyba że przepisy szczególne stanowią inaczej.	
Art. 91	**Istniejące zasady ochrony danych obowiązujące kościoły i związki wyznaniowe** 1. Jeżeli w państwie członkowskim w momencie wejścia niniejszego rozporządzenia w życie kościoły i związki lub wspólnoty wyznaniowe stosują szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem, zasady takie mogą być nadal stosowane, pod warunkiem że zostaną dostosowane do niniejszego rozporządzenia. 2. Kościoły i związki wyznaniowe, które stosują szczegółowe zasady zgodnie z ust. 1 niniejszego artykułu, podlegają nadzorowi niezależnego organu nadzorczego, który może być organem odrębnym, z zastrzeżeniem że spełnia warunki określone w rozdziale VI niniejszego rozporządzenia.	**N**			
ROZDZIAŁ X **AKTY DELEGOWANE I AKTY WYKONAWCZE**					
Art. 92	**Wykonywanie przekazanych uprawnień** 1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule. 2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 12 ust. 8 i art. 43 ust. 8, powierza się Komisji na czas nieokreślony od dnia 24 maja 2016 r. 3. Przekazanie uprawnień, o którym mowa w art. 12. ust. 8 i art. 43 ust. 8, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych. 4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.	**N**			

	5. Akt delegowany przyjęty na podstawie art. 12 ust. 8 i art. 43 ust. 8 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.				
Art. 93	**Procedura komitetowa** 1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011. 2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011. 3. W przypadku odesłania do niniejszego ustępu stosuje się art. 8 rozporządzenia (UE) nr 182/2011 w związku z jego art. 5.	**N**			
ROZDZIAŁ XI **PRZEPISY KOŃCOWE**					
Art. 94	**Uchylenie dyrektywy 95/46/WE** 1. Dyrektywa 95/46/WE zostaje uchylona ze skutkiem od dnia 25 maja 2018 r. 2. Odesłania do uchylonej dyrektywy należy traktować jako odesłania do niniejszego rozporządzenia. Odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy 95/46/WE, należy traktować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej niniejszym rozporządzeniem	**N**			
Art. 95	**Stosunek do dyrektywy 2002/58/WE** Niniejsze rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie 2002/58/WE.	**N**			
Art. 96	**Stosunek do uprzednio zawartych umów** Umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed dniem 24 maja 2016 r., i które są zgodne z prawem Unii mającym zastosowanie przed tym dniem, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.	**N**			

Art. 97	**Sprawozdania Komisji** 1. Do dnia 25 maja 2020 r., a następie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdania z oceny i przeglądu niniejszego rozporządzenia. Sprawozdania te są podawane do wiadomości publicznej. 2. W ramach tych ocen Komisja analizuje i dokonuje przeglądu, o którym mowa w ust. 1, w szczególności stosowania i funkcjonowania przepisów: a) rozdziału V dotyczącego przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych ze szczególnym uwzględnieniem decyzji przyjętych na mocy art. 45 ust. 3 niniejszego rozporządzenia oraz decyzji przyjętych na podstawie art. 25 ust. 6 dyrektywy 95/46/WE; b) rozdziału VII dotyczącego współpracy i spójności. 3. Na potrzeby ust. 1, Komisja może wystąpić do państw członkowskich i organów nadzorczych o udzielenie informacji. 4. Dokonując ocen i przeglądów, o których mowa w ust. 1 i 2, Komisja uwzględnia stanowiska i ustalenia Parlamentu Europejskiego, Rady oraz innych stosownych podmiotów lub źródeł. 5. W razie potrzeby Komisja przedkłada odpowiednie wnioski przewidujące zmianę niniejszego rozporządzenia, uwzględniając w szczególności rozwój technologii informacyjnych oraz postęp w społeczeństwie informacyjnym.	**N**			
Art. 98	**Przegląd innych aktów prawnych Unii dotyczących ochrony danych** Komisja przedkłada w stosownym przypadku wnioski ustawodawcze dotyczące zmiany innych aktów prawnych Unii dotyczących ochrony danych osobowych, aby zapewnić jednolitą i spójną ochronę osób fizycznych w związku z przetwarzaniem. Dotyczy to w szczególności przepisów o ochronie osób fizycznych w związku z przetwarzaniem przez instytucje, organy i jednostki organizacyjne Unii oraz o swobodnym przepływie danych osobowych.	**N**			
Art. 99	**Wejście w życie i stosowanie** 1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po publikacji w *Dzienniku Urzędowym Unii Europejskiej*. 2. Niniejsze rozporządzenie ma zastosowanie od dnia 25 maja 2018 r. Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.	**N**			

Warszawa, 4 kwietnia 2018 r.

[redacted]

Minister
Spraw Zagranicznych

DPUE.920.1409.2017/68/mp

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

Pani
Jolanta Rusiniak
Sekretarz Rady Ministrów

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

Szanowna Pani Minister,

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

1. Na podstawie art. 5 ust. 2 projektu ustawy wnioskodawca wprowadza ograniczenie stosowania art. 15 ust. 1 i 3 *rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych; RODO). Ograniczenie to polega na wprowadzeniu obowiązku wskazania przez osobę, której dane dotyczą, informacji pozwalających na wyszukanie jej danych osobowych w przypadku, gdy takie wyszukanie wymaga niewspółmiernie dużego wysiłku.

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

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

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

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

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

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

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

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

a) w ramach działalności nieobjętej prawem UE;

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

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

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

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

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

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

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

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

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

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

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

Uwzględniając powyższe proponuję usunąć art. 97 z projektu ustawy.

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

Z poważaniem

z up. Ministra Spraw Zagranicznych
Piotr Wawrzyk
Podsekretarz Stanu

Do wiadomości:
Pan Marek Zagórski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Projekt ustawy o ochronie danych osobowych

Etap: RM

Projekt wykonuje rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; dalej: RODO)

Termin wdrożenia: 25 maja 2018 r.

Resort wnoszący: Ministerstwo Cyfryzacji

Minister odpowiedzialny za projekt ustawy: Sekretarz Stanu Marek Zagórski

---

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

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

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

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

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

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych

Na podstawie art. 48 ustawy z dnia ... o ochronie danych osobowych (Dz. U. poz. ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa wzór legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych, zwanego dalej „pracownikiem”.

§ 2. Wzór legitymacji służbowej pracownika określa załącznik do rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

Załącznik
do rozporządzenia
Rady Ministrów
z dnia ... (poz. ...)

LEGITYMACJA SŁUŻBOWA PRACOWNIKA URZĘDU OCHRONY DANYCH OSOBOWYCH

(WZÓR)

OPIS:

awers legitymacji:

– legitymacja koloru niebieskiego,
– napisy w kolorze czarnym: Rzeczpospolita Polska, Urząd Ochrony Danych Osobowych,
– numer legitymacji,
– orzeł z godła RP,
– pasek przekątny koloru biało-czerwonego;

rewers legitymacji:
– legitymacja koloru niebieskiego,
– napisy w kolorze czarnym: LEGITYMACJA SŁUŻBOWA pracownika Urzędu Ochrony Danych Osobowych, ważna do, miejsce na fotografię, miejsce na pieczęć, nazwisko, imię, nr ewidencyjny PESEL, (podpis wystawcy), (podpis właściciela),
– hologram z literami w kolorze niebieskim;

wymiary legitymacji:
– wysokość legitymacji 90 mm,
– szerokość legitymacji 65 mm,
– wysokość fotografii 35 mm
– szerokość fotografii 25 mm;
– rodzaj papieru i zabezpieczeń:
– gramatura papieru 200,
– papier kredowany dwustronnie – matowy,
– hologram,
– w miejscach wpisu nazwiska i imienia oraz numeru ewidencyjnego PESEL nadruk cienkich linii zabezpieczających.

UZASADNIENIE

Projektowane rozporządzenie wykonuje delegację ustawową zawartą w art. 48 ustawy o ochronie danych osobowych (Dz. U. poz. …), zgodnie z którym Rada Ministrów została upoważniona do określenia wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych.

Wzór legitymacji określa załącznik do rozporządzenia.

Projekt nie jest objęty przepisami prawa Unii Europejskiej.

Projekt nie zawiera przepisów technicznych, w związku z tym nie wymaga notyfikacji technicznej, o której mowa w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji oraz Rządowego Centrum Legislacji.

Nazwa projektu	**Data sporządzenia**
Rozporządzenie Rady Ministrów w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych	
Ministerstwo wiodące i ministerstwa współpracujące	**Źródło:**
Ministerstwo Cyfryzacji	Art. 48 ustawy z dnia … o ochronie danych osobowych
Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu	
Marek Zagórski – Sekretarz Stanu w Ministerstwie Cyfryzacji	**Nr w wykazie prac …….**
Kontakt do opiekuna merytorycznego projektu	
Maciej Kawecki – Dyrektor Departamentu Zarządzania Danymi	

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Konieczność przygotowania przedmiotowego rozporządzenia wynika z faktu, iż ustawa z dnia … o ochronie danych osobowych (Dz. U. poz. …), zwana dalej „ustawą”, przewiduje w art. 48 wydanie rozporządzenia określającego wzór legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych. Wydając rozporządzenie Rada Ministrów winna mieć na względzie potrzebę zapewnienia możliwości identyfikacji osób uprawnionych do przeprowadzenia kontroli oraz wykonywania innych czynności służbowych.

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

Nie dotyczy.

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

Wydanie rozporządzenia w sprawie legitymacji pozwoli na określenie wzoru legitymacji dla pracowników Urzędu Ochrony Danych Osobowych, zwanego dalej „Urzędem”, a tym samym umożliwi im realizację ich ustawowych zadań, tj. przeprowadzanie kontroli administratorów danych lub podmiotów przetwarzających w przypadkach określonych w ustawie.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Pracownicy Urzędu Ochrony Danych Osobowych	Ok. 151 osób	Dane zawarte w sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z 2016 r., opublikowanego na stronie internetowej GIODO, gdzie liczba pracowników na dzień 31 grudnia 2016 r. wyniosła 151,525 etatu	Wyprodukowanie i wyposażenie w legitymacje

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

Projekt rozporządzenia zostanie zamieszczony w Biuletynie Informacji Publicznej na stronie Rządowego Centrum Legislacji, w Biuletynie Informacji Publicznej na stronie Ministra Cyfryzacji, a informacja o konsultacjach została opublikowana na stronie Ministerstwa Cyfryzacji. Konsultacje trwały 21 dni i były dostępne dla wszystkich zainteresowanych osób.

Projekt został także skierowany do następujących podmiotów:

1. Polskiego Towarzystwa Informatycznego (PTI),
2. Polskiej Izby Informatyki i Telekomunikacji (PIIT),
3. Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (KIGEiT),
4. Stowarzyszenia Instytutu Informatyki Śledczej,
5. Polskiego Komitetu Normalizacyjnego (PKN),
6. Związku Pracodawców Branży Internetowej Interactive Advertising Bureau Polska,
7. Konfederacji Lewiatan,
8. Związku Rzemiosła Polskiego,
9. Ogólnopolskiego Porozumienia Związków Zawodowych,

10. Forum Związków Zawodowych,
11. Pracodawców RP,
12. Business Centre Club,
13. NSZZ Solidarność,
14. Fundacji Panoptykon,
15. Polskiej Izby Komunikacji Elektronicznej,
16. Internet Society Poland,
17. Zakładu Ubezpieczeń Społecznych (ZUS),
18. Rady Głównej Instytutów Badawczych (RGIB),
19. Instytutu Logistyki i Magazynowania (ILiM).

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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem		0,0031	0	0	0	0	0	0	0	0	0	0,0031
budżet państwa		0,0031	0	0	0	0	0	0	0	0	0	0,0031
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem		-0,0031	0	0	0	0	0	0	0	0	0	-0,0031
budżet państwa		-0,0031	0	0	0	0	0	0	0	0	0	-0,0031
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Budżet państwa, cz. 10
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Zgodnie z art. 159 ustawy dotychczasowe przepisy wykonawcze wydane na podstawie art. 22a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 i z 2018 r. poz. 138) zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 48 ustawy, nie dłużej niż 12 miesięcy od dnia wejścia w życie ustawy. W efekcie należy przyjąć, że od początku 2019 r. nastąpi sukcesywne wydawanie nowych legitymacji. Do obliczeń przyjęto średni koszt wyprodukowania i dostarczenia jednej legitymacji w wysokości ok. 20,00 zł. W celu oszacowania całkowitego kosztu wyposażenia pracowników Urzędu w legitymacje, pomnożono koszt jednej legitymacji przez przybliżoną liczbę pracowników, tj. 151 osób, uzyskując kwotę w wysokości ok. 3100,00 zł. Dodatkowo przyjęto założenie, zgodnie z którym koszt wyprodukowania legitymacji dla 151 pracowników zostanie poniesiony w 2019 r. Jednocześnie mając na uwadze fluktuacje kadr, koszt wyposażenia pracowników w legitymacje może przedstawiać się różnie w kolejnych latach, dlatego też jest trudny do oszacowania. Środki na wyprodukowanie i dostarczenie legitymacji dla pracowników Urzędu będą pochodziły ze środków będących w dyspozycji Prezesa Urzędu.

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							Nie dotyczy.
	sektor mikro-, małych i średnich przedsiębiorstw							Nie dotyczy.
	rodzina, obywatele oraz gospodarstwa domowe							Nie dotyczy.
W ujęciu niepieniężnym	duże przedsiębiorstwa	Nie dotyczy.						
	sektor mikro-, małych i średnich przedsiębiorstw	Nie dotyczy.						
	rodzina, obywatele oraz gospodarstwa domowe	Nie dotyczy.						
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy.

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:
Nie dotyczy.

9. Wpływ na rynek pracy

Nie dotyczy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Nie dotyczy.
11. Planowane wykonanie przepisów aktu prawnego	
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?	
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)	

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I T R Ó W

z dnia

w sprawie wysokości wynagrodzenia członków Rady do Spraw Ochrony Danych Osobowych oraz liczby jej posiedzeń w roku kalendarzowym

Na podstawie art. 50 ust. 3 ustawy z dnia … o ochronie danych osobowych (Dz. U. poz. ...) zarządza się, co następuje:

§ 1. Członkowie Rady do Spraw Ochrony Danych Osobowych, zwanej dalej „Radą”, w związku z wykonywaniem swoich obowiązków otrzymują za udział w posiedzeniu Rady wynagrodzenie w wysokości:

1) po 400 zł – Przewodniczący i Wiceprzewodniczący Rady;
2) po 350 zł – pozostali członkowie Rady.

§ 2. Wynagrodzenie, o którym mowa w § 1, przysługuje za każde z 12 posiedzeń Rady w roku kalendarzowym. Za każde następne posiedzenie wynagrodzenie nie przysługuje.

§ 3. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

UZASADNIENIE

Projektowane rozporządzenie wykonuje delegację ustawową zawartą w art. 50 ust. 3 ustawy z dnia … o ochronie danych osobowych (Dz. U. poz. ...).

Konieczność przygotowania przedmiotowego rozporządzenia wynika z faktu, iż ww. ustawa przewiduje powołanie przy Prezesie Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu", działa Rada do Spraw Ochrony Danych Osobowych, zwana dalej „Radą", która jest organem opiniodawczo-doradczym Prezesa Urzędu. Do zadań Rady należy:

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

Rada składa się z 8 członków. Powołanie do Rady następuje na dwuletnią kadencję spośród kandydatów. Obsługę Rady zapewnia Urząd Prezesa a szczegółowy tryb działania Rady określa regulamin ustanawiany na wniosek Rady przez Prezesa Urzędu.

Jednocześnie z uwagi na zakres zadań Rady, ustawa w art. 50 przewiduje, że za udział w pracach Rady członkowi przysługuje wynagrodzenie. Wysokość wynagrodzenia uzależniona jest od zakresu obowiązków związanych z funkcją pełnioną w Radzie oraz liczby posiedzeń w których uczestniczył. Jednocześnie ustawodawca wskazał, że wynagrodzenie członka Rady za jedno posiedzenie stanowi co najmniej 5% przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok powołania Rady, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 20 pkt 1 lit. a

ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych i nie może przekroczyć 25% tego wynagrodzenia.

Niniejsze rozporządzenie realizuje upoważnienie do wydania przez Radę Ministrów rozporządzenia do określenia wysokości wynagrodzenia członka Rady za udział w posiedzeniu. Projekt rozporządzenia określa także liczbę posiedzeń Rady w ciągu roku kalendarzowego, za które przysługuje członkom Rady wynagrodzenie.

Projekt nie jest objęty przepisami prawa Unii Europejskiej.

Projekt nie zawiera przepisów technicznych, w związku z tym nie wymaga notyfikacji technicznej, o której mowa w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji oraz Rządowego Centrum Legislacji.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie wysokości wynagrodzenia członków Rady do Spraw Ochrony Danych Osobowych oraz liczby jej posiedzeń w roku kalendarzowym **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Marek Zagórski – Sekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Maciej Kawecki – Dyrektor Departamentu Zarządzania Danymi	**Data sporządzenia** **Źródło:** Art. 50 ust. 3 ustawy z dnia … o ochronie danych osobowych **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Konieczność przygotowania przedmiotowego rozporządzenia wynika z faktu, iż ww. ustawa przewiduje powołanie przy Prezesie Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu", działa Rada do Spraw Ochrony Danych Osobowych, zwana dalej „Radą", która jest organem opiniodawczo-doradczym Prezesa Urzędu.
Niniejsze rozporządzenie realizuje upoważnienie do wydania przez Radę Ministrów rozporządzenia do określenia wysokości wynagrodzenia członka Rady za udział w posiedzeniu (art. 50 ust. 3). Projekt rozporządzenia określa także liczbę posiedzeń Rady w ciągu roku kalendarzowego, za które przysługuje członkom Rady wynagrodzenie.

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

Wobec zaangażowania się członków Rady w jej prace proponuje się przyznanie wynagrodzenia za udział w pracach Rady, co zapewni realną pomoc Prezesowi Urzędu w wypełnianiu zadań określonych w ustawie.

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

Konieczność zrealizowania upoważnienia z art. 50 ust. 3 ustawy z dnia … o ochronie danych osobowych, nakładającego na Radę Ministrów obowiązek wydania rozporządzenia określającego wysokość wynagrodzenia członków Rady do Spraw Ochrony Danych Osobowych oraz liczby jej posiedzeń w roku kalendarzowym.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Członkowie Rady do Spraw Ochrony Danych Osobowych	8	Art. 50 ustawy	Określenie wysokości wynagrodzenia

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

Projekt rozporządzenia zostanie umieszczony w Biuletynie Informacji Publicznej RCL, w Biuletynie Informacji Publicznej na stronie Ministra Cyfryzacji, a informacja o konsultacjach została opublikowana na stronie Ministerstwa. Konsultacje trwały 21 dni i były dostępne dla wszystkich zainteresowanych osób.
Projekt został także skierowany do następujących podmiotów:

- Polskiego Towarzystwa Informatycznego (PTI),
- Polskiej Izby Informatyki i Telekomunikacji (PIIT),
- Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (KIGEiT),
- Stowarzyszenia Instytutu Informatyki Śledczej,
- Polskiego Komitetu Normalizacyjnego (PKN),
- Związku Pracodawców Branży Internetowej Interactive Advertising Bureau Polska,
- Konfederacji Lewiatan,
- Związku Rzemiosła Polskiego,
- Ogólnopolskiego Porozumienia Związków Zawodowych,
- Forum Związków Zawodowych,
- Pracodawców RP,
- Business Centre Club,
- NSZZ Solidarność,
- Fundacji Panoptykon,
- Polskiej Izby Komunikacji Elektronicznej,
- Internet Society Poland,

- Zakładu Ubezpieczeń Społecznych (ZUS),
- Rady Głównej Instytutów Badawczych (RGIB),
- Instytutu Logistyki i Magazynowania (ILiM).

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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem	0,02	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,32
budżet państwa	0,02	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,32
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	-0,02	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,32
budżet państwa	-0,02	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,03	-0,32
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Budżet państwa część 10-Generalny Inspektor Danych Osobowych
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wejście w życie rozporządzenia nie będzie wywoływać dodatkowych skutków finansowych dla budżetu państwa innych niż określonych w ustawie o ochronie danych osobowych. Za rok bazowy w pkt 6 OSR „(O)" przyjęto 2018 r., czyli rok wejścia w życie ustawy. Wydatki wykazane w zestawieniu tabelarycznym oszacowano w 2018 r. proporcjonalnie za 7 miesięcy tj. od VI do XII 2018 r. Art. 50 ustawy z dnia … o ochronie danych osobowych wynika, że wynagrodzenie członków rady może stanowić od 5 do 25 procent przeciętnego wynagrodzenia w gospodarce narodowej w roku kalendarzowym poprzedzającym rok powołania Rady, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. Przyjęto Komunikat Prezesa Głównego Urzędu Statystycznego z dnia 9 lutego 2018 r. w sprawie przeciętnego wynagrodzenia w gospodarce narodowej w 2017 r. w którym określono przeciętne wynagrodzenie w gospodarce narodowej w 2017 r. w wysokości 4271,51 zł. Kwota 400 i 350 złotych stanowią odpowiednią ok. 8 i 9 procent kwoty 4271,51 zł wynikającej z ww. komunikatu. W ocenie projektodawcy ok. 10 procent wynagrodzenia członków rady stanowi odpowiednią motywację dla członków rady do zaangażowania się w pracę Rady. Przyjmując, że Rada do Spraw Ochrony Danych Osobowych spotykałaby się raz w miesiąc, łączny roczny koszt wynagrodzeń jej 8 członków wyniósłby ok. 34 200,00 zł. Należy wskazać, że członkom Rady posiadającym miejsce zamieszkania poza siedzibą Prezesa Urzędu będą przysługiwać, zgodnie z art. 50 ust. 4 ustawy diety oraz zwrot kosztów podróży i zakwaterowania na warunkach określonych w przepisach wydanych na podstawie art. 77^5 § 2 ustawy z dnia 26 czerwca 1974 r. − Kodeks pracy (Dz. U. z 2018 r. poz. 108, 138, 305 i 357). Wydatki dotyczące zwrotu kosztów i diet ww. zostały ujęte w Ocenie Skutków Regulacji dołączonej do projektu ustawy o ochronie danych osobowych.

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							Nie dotyczy.
	sektor mikro-, małych i średnich przedsiębiorstw							Nie dotyczy.
	rodzina, obywatele oraz gospodarstwa domowe							Nie dotyczy.
W ujęciu niepieniężnym	duże przedsiębiorstwa	Nie dotyczy.						
	sektor mikro-, małych i średnich przedsiębiorstw	Nie dotyczy.						
	rodzina, obywatele oraz gospodarstwa domowe	Nie dotyczy.						
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy.

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:

Nie dotyczy.

9. Wpływ na rynek pracy

Nie dotyczy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Nie dotyczy.

11. Planowane wykonanie przepisów aktu prawnego

Planowany termin wejścia w życie projektowanego rozporządzenia 25 maja 2018 r.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
Nie dotyczy.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Brak załączników.