Projekt

U S T A W A

z dnia

o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[1), 2)]

Rozdział 1

Przepisy ogólne

---

1) Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia 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).

2) Niniejszą ustawą zmienia się następujące ustawy: ustawę z dnia 26 marca 1982 r. o Trybunale Stanu, ustawę z dnia 18 kwietnia 1985 r. o rybactwie śródlądowym, ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, ustawę z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska, ustawę z dnia 28 września 1991 r. o lasach, ustawę z dnia 13 października 1995 r. – Prawo łowieckie, ustawę z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, ustawę z dnia 10 kwietnia 1997 r. – Prawo energetyczne, ustawę z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy, ustawę z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych, ustawę z dnia 29 sierpnia 1997 r. o strażach gminnych, ustawę z dnia 21 grudnia 2000 r. o żegludze śródlądowej, ustawę z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, ustawę z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 6 września 2001 r. o transporcie drogowym, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych, ustawę z dnia 28 marca 2003 r. o transporcie kolejowym, ustawę z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawę z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, ustawę z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, ustawę z dnia 9 kwietnia 2010 r. o Służbie Więziennej, ustawę z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, ustawę z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, ustawę z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym, ustawę z dnia 28 stycznia 2016 r. – Prawo o prokuraturze, 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 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym, ustawę z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami, ustawę z dnia 20 lipca 2017 r. – Prawo wodne, ustawę z dnia 8 grudnia 2017 r. o Sądzie Najwyższym, ustawę z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, ustawę z dnia 10 stycznia 2018 r. o szczególnych rozwiązaniach związanych z organizacją w Rzeczypospolitej Polskiej sesji Konferencji Stron Ramowej konwencji Narodów Zjednoczonych w sprawie zmian klimatu, ustawę z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej, ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz ustawę z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera.

Art. 1. Ustawa określa:

1) zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności;
2) prawa osób, których dane osobowe są przetwarzane przez właściwe organy w celach, o których mowa w pkt 1, oraz środki ochrony prawnej przysługujące tym osobom;
3) sposób prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez właściwe organy w celach, o których mowa w pkt 1, z wyłączeniem danych osobowych przetwarzanych przez prokuraturę i sądy;
4) zadania organu nadzorczego oraz formy i sposób ich wykonania;
5) obowiązki administratora i podmiotu przetwarzającego oraz inspektora ochrony danych i tryb jego wyznaczania;
6) sposób zabezpieczenia danych osobowych;
7) tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej;
8) odpowiedzialność karną za naruszenie przepisów niniejszej ustawy.

Art. 2. Ustawę stosuje się do przetwarzania danych osobowych przez właściwe organy w celach, o których mowa w art. 1 pkt 1, w sposób:

1) całkowicie lub częściowo zautomatyzowany;
2) inny niż zautomatyzowany, w przypadku gdy dane te stanowią lub mają stanowić część zbioru danych.

Art. 3. Przepisów ustawy nie stosuje się do ochrony danych osobowych:

1) znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2018 r. poz. 969), ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652, 1010 i 1387), ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2017 r. poz. 1904, z późn. zm.[3)]), ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U.

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 5, 106, 138, 201, 730, 771, 942, 1387 i 1467.

z 2017 r. poz. 2226 oraz z 2018 r. poz. 201 i 771), ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475, 1039, 1387, 1467 i 1481), ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396 oraz z 2016 r. poz. 2205), ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5, 1000, 1443 i 1669) oraz wydanych na ich podstawie aktów wykonawczych;

2) przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego.

Art. 4. Ilekroć w ustawie jest mowa o:

1) administratorze – rozumie się przez to właściwy organ, który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych, podmiot wskazany przez ustawę jako administrator, jeżeli cele i sposoby przetwarzania danych osobowych są określone w ustawie, albo podmiot wskazany przez prawo Unii Europejskiej albo prawo państwa członkowskiego lub podmiot wyznaczony zgodnie z kryteriami określonymi w prawie tego państwa;
2) danych biometrycznych – rozumie się przez to dane osobowe dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, w tym wizerunek twarzy lub dane daktyloskopijne, które zostały uzyskane wskutek specjalnego przetwarzania technicznego;
3) danych dotyczących zdrowia – rozumie się przez to dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym dane o korzystaniu z usług opieki zdrowotnej, które ujawniają informacje o stanie jej zdrowia;
4) danych genetycznych – rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które zostały uzyskane w szczególności z analizy próbki biologicznej pochodzącej od tej osoby;
5) danych osobowych – rozumie się przez to dane osobowe, o których mowa w art. 4 pkt 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 osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[4)]);

6) naruszeniu ochrony danych osobowych – rozumie się przez to 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;

7) odbiorcy – rozumie się przez to osobę fizyczną lub prawną, organ administracji publicznej, jednostkę organizacyjną lub inny podmiot, któremu ujawnia się dane osobowe, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, a przetwarzanie tych danych jest zgodne z przepisami o ochronie danych mającymi zastosowanie do ich celów przetwarzania;

8) ograniczeniu przetwarzania – rozumie się przez to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

9) organie nadzorczym w innych państwach Unii Europejskiej – rozumie się przez to niezależny organ publiczny ustanowiony przez inne niż Rzeczpospolita Polska państwo członkowskie Unii Europejskiej, powołany dla ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej;

10) organizacji międzynarodowej – rozumie się przez to 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;

11) organach ścigania państw członkowskich Unii Europejskiej – rozumie się przez to organy państw członkowskich Unii Europejskiej oraz państw niebędących państwami członkowskimi Unii Europejskiej stosujących przepisy dorobku Schengen, które są

[4)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L127 z 23.05.2018, str. 2.

uprawnione w tych państwach do wykrywania i ścigania sprawców przestępstw lub przestępstw skarbowych oraz zapobiegania przestępczości i jej zwalczania;

12) państwie trzecim – rozumie się przez to państwo niebędące państwem członkowskim Unii Europejskiej i niestosujące przepisów dorobku Schengen;

13) podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ władzy publicznej, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

14) profilowaniu – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na ich wykorzystaniu do oceny niektórych cech osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

15) przetwarzaniu – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

16) pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, aby 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;

17) właściwym organie – rozumie się przez to organ władzy publicznej, jednostkę organizacyjną lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych;

18) wymianie – rozumie się przez to przekazywanie, udostępnianie lub otrzymywanie informacji przez organy ścigania państw członkowskich Unii Europejskiej, państw trzecich lub agencje Unii Europejskiej i organizacje międzynarodowe zajmujące się zapobieganiem i zwalczaniem przestępczości oraz organy nadzorcze Unii Europejskiej, o których mowa w art. 48 i art. 49;

19) zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rozdział 2

Zadania organu nadzorczego

Art. 5. 1. Do zadań Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu”, należy:

1) monitorowanie i egzekwowanie stosowania przepisów niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych;
2) upowszechnianie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych w celu, o którym mowa w art. 1 pkt 1, oraz rozumieniem tych zjawisk;
3) doradzanie instytucjom publicznym w sprawach środków ochrony praw i wolności osób fizycznych z związku z przetwarzaniem danych osobowych w celu, o którym mowa w art. 1 pkt 1;
4) upowszechnianie wiedzy z zakresu stosowania niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych wśród administratorów i podmiotów przetwarzających;
5) udzielanie osobie, której dane dotyczą, na jej żądanie, informacji o wykonywaniu praw przysługujących jej na mocy niniejszej ustawy, a w miarę potrzeby współpracowanie w tym celu z organami nadzorczymi w innych państwach Unii Europejskiej;
6) rozpatrywanie skarg osób, których dane osobowe są przetwarzane niezgodnie z prawem, i prowadzenie postępowań w tym zakresie;
7) o ile przepis szczególny nie stanowi inaczej, kontrola zgodności przetwarzania danych osobowych z przepisami niniejszej ustawy;
8) prowadzenie postępowania w sprawie stosowania niniejszej ustawy, w tym na podstawie informacji otrzymanych od innego organu publicznego;
9) pełnienie funkcji konsultacyjnych, o których mowa w art. 38, dotyczących operacji przetwarzania w ramach niniejszej ustawy;
10) współpraca z organami nadzorczymi w państwach członkowskich Unii Europejskiej;
11) wydawanie opinii dla Sejmu, Senatu oraz innych organów władzy publicznej w sprawach ochrony danych osobowych;

12) wydawanie opinii w odniesieniu do projektów aktów prawnych w sprawach dotyczących ochrony danych osobowych.

2. Jeżeli żądanie wykonania zadania jest w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swoją powtarzalność, Prezes Urzędu może pobrać opłatę, której wysokość odpowiada przewidywanym kosztom poniesionym z tytułu wykonywania zadania, lub może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na Prezesie Urzędu. Prezes Urzędu podejmuje działania po pobraniu opłaty. Opłata pobrana przez Prezesa Urzędu stanowi dochód budżetu państwa.

3. Założenia i projekty ustaw i rozporządzeń dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu.

Art. 6. W celu wykonania zadań, o których mowa w art. 5 ust. 1 pkt 1 i 6–8, Prezes Urzędu może przeprowadzać kontrolę przetwarzania danych osobowych, zwaną dalej „kontrolą”. Do prowadzenia kontroli stosuje się odpowiednio przepisy rozdziału 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669), z wyłączeniem art. 79 ust. 1 pkt 2, art. 83, art. 84 ust. 4 i art. 85 tej ustawy.

Art. 7. W toku kontroli upoważniony przez Prezesa Urzędu pracownik Urzędu Ochrony Danych Osobowych, zwany dalej „kontrolującym”, ma prawo wglądu do zbioru danych podlegającego kontroli oraz do innych dokumentów mających bezpośredni związek z przedmiotem kontroli. Kontrolujący ma prawo wglądu do zbioru danych oraz do innych dokumentów, o których mowa w zdaniu pierwszym, jedynie w obecności upoważnionego przedstawiciela właściwego organu, w którym jest prowadzona kontrola.

Art. 8. 1. W przypadku uzasadnionego podejrzenia, że planowane operacje przetwarzania mogą skutkować naruszeniem przepisów niniejszej ustawy, Prezes Urzędu wydaje administratorowi lub podmiotowi przetwarzającemu ostrzeżenie.

2. W przypadku naruszenia przepisów o ochronie danych osobowych zbieranych w celach, o których mowa w art. 1 pkt 1, Prezes Urzędu, w drodze decyzji administracyjnej, nakazuje administratorowi lub podmiotowi przetwarzającemu przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień;
2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;

3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;
4) zabezpieczenie danych osobowych lub przekazanie ich innym podmiotom;
5) usunięcie danych osobowych;
6) wprowadzenie czasowych lub stałych ograniczeń przetwarzania i przekazywania, w tym zakazu przetwarzania.

3. Decyzje Prezesa Urzędu, o których mowa w ust. 1, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Administrator w przypadku uznania, że zgromadzone w ten sposób dane są zbędne, jest zobowiązany do ich usunięcia. W przypadku niedopełnienia obowiązku usunięcia danych osobowych przez administratora Prezes Urzędu może nakazać ich usunięcie. W celu realizacji uprawnienia Prezes Urzędu nie uzyskuje dostępu do danych osobowych, o których mowa w zdaniu pierwszym. Administrator lub podmiot przetwarzający dane osobowe, o których mowa w zdaniu pierwszym, jest zobowiązany do niezwłocznego przywrócenia zgodnego z prawem sposobu ich przetwarzania.

Art. 9. 1. Postępowanie w sprawach, o których mowa w art. 8 ust. 2, jest jednoinstancyjne.

2. Na decyzję Prezesa Urzędu, o której mowa w art. 8 ust. 2, przysługuje skarga do sądu administracyjnego.

Art. 10. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1 pkt 5 i 10, Prezes Urzędu może kierować do administratora lub podmiotu przetwarzającego wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych zbieranych w celach, o których mowa w art. 1 pkt 1.

2. Podmiot, do którego zostało skierowane wystąpienie, o którym mowa w ust. 1, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku pisemnie w postaci papierowej lub elektronicznej w terminie 30 dni od daty jego otrzymania.

Art. 11. 1. Prezes Urzędu może zwrócić się bezpośrednio do inspektora ochrony danych, o którym mowa w art. 46, o przeprowadzenie sprawdzenia stosowania przepisów niniejszej ustawy przez administratora, który go wyznaczył, wskazując zakres i termin tego sprawdzenia.

2. Po przeprowadzeniu audytu, o którym mowa w ust. 1, inspektor ochrony danych, za pośrednictwem administratora, przedstawia Prezesowi Urzędu sprawozdanie z przeprowadzonego sprawdzenia.

3. Przeprowadzenie przez inspektora ochrony danych sprawdzenia w przypadku, o którym mowa w ust. 1, nie wyłącza prawa Prezesa Urzędu do przeprowadzenia kontroli, o której mowa w art. 7.

Art. 12. Postępowanie w sprawach objętych zakresem regulacji niniejszego rozdziału prowadzi się według przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149, 650, 1544 i 1629), zwanej dalej „Kodeksem postępowania administracyjnego”, o ile przepisy niniejszej ustawy nie stanowią inaczej.

Rozdział 3

Zasady dotyczące przetwarzania danych osobowych

Art. 13. 1. Właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

2. Dopuszcza się przetwarzanie danych osobowych zebranych pierwotnie w jednym z celów, o których mowa w art. 1 pkt 1, w innych nowych celach, o których mowa w art. 1 pkt 1, o ile:

1) administratorowi wolno przetwarzać takie dane osobowe w innym nowym celu na mocy odrębnych przepisów;
2) przetwarzanie jest niezbędne i proporcjonalne w tym innym nowym celu na mocy odrębnych przepisów.

3. Dopuszcza się przetwarzanie danych osobowych do innych celów niż określone w art. 1 pkt 1, jeżeli przepisy prawa, w tym prawa Unii Europejskiej, zezwalają na ich przetwarzanie.

4. Dopuszcza się wykorzystanie przetwarzania danych osobowych zebranych do celów, o których mowa w art. 1 pkt 1, w zakresie niezbędnym do ich archiwizacji w interesie publicznym oraz do celów naukowych, statystycznych lub historycznych, o ile podlega ono odpowiednim zabezpieczeniom praw i wolności osób, których dane dotyczą.

Art. 14. 1. Niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych

dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej, zwanych dalej „danymi wrażliwymi”.

2. Dopuszcza się przetwarzanie danych wrażliwych, jeżeli:

1) przepisy prawa, w tym prawa Unii Europejskiej, zezwalają na ich przetwarzanie lub
2) jest to niezbędne dla ochrony życia lub zdrowia interesów osoby, której dane dotyczą, lub innej osoby, lub
3) dane takie zostały upublicznione przez osobę, której dotyczą.

Art. 15. 1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, mające dla niej niekorzystne skutki prawne lub poważnie na nią wpływające, wyłącznie w wyniku przetwarzania danych osobowych w sposób zautomatyzowany, w tym w wyniku profilowania, chyba że dopuszcza je prawo Unii Europejskiej lub odrębne przepisy, którym podlega administrator i które przewidują odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ze strony administratora.

2. Rozstrzygnięcia, o których mowa w ust. 1, nie mogą opierać się na danych wrażliwych, chyba że istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.

3. Niedopuszczalne jest dokonywanie profilowania osób fizycznych na podstawie danych wrażliwych, skutkującego dyskryminacją tych osób.

Art. 16. 1. Administrator dokonuje weryfikacji danych osobowych w terminach określonych przez przepisy szczególne, regulujące działania właściwego organu, a jeżeli przepisy te nie określają terminu – nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych.

2. Weryfikacja dokonywana jest w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane usuwa się, z zastrzeżeniem art. 17.

Art. 17. Dane osobowe uznane za zbędne można przekształcić w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań.

Art. 18. Jeżeli dane osobowe są przetwarzane w związku z dokumentowaniem czynności realizowanych przez właściwe organy, jako elektroniczna kopia akt kontrolnych, dane pozostawia się po ich zanonimizowaniu.

Art. 19. Przy przetwarzaniu danych osobowych administrator zapewnia rozróżnienie, o ile jest ono możliwe lub nie jest dalece utrudnione, na dane osobowe dotyczące:

1) osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
2) osób skazanych za czyn zabroniony;
3) pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;
4) innych osób związanych z czynem zabronionym, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w pkt 1 i 2.

Art. 20. Przy przetwarzaniu danych osobowych administrator zapewnia rozróżnienie, o ile jest ono możliwe lub nie jest dalece utrudnione, na dane osobowe mające swoje źródło w faktach i dane osobowe mające swoje źródło w indywidualnych ocenach.

Art. 21. 1. Właściwy organ może przesyłać lub udostępniać dane osobowe innym właściwym organom, państwu trzeciemu lub organizacji międzynarodowej po uprzednim zweryfikowaniu, w miarę potrzeby i możliwości, prawidłowości, kompletności i aktualności tych danych.

2. Właściwy organ, przesyłając dane osobowe odbiorcom, o których mowa w ust. 1, przekazuje, w miarę potrzeby i możliwości, niezbędne dodatkowe informacje pozwalające odbiorcy ocenić stopień prawidłowości, kompletności oraz aktualności przesłanych danych osobowych.

3. Właściwy organ, który przesłał odbiorcom, o których mowa w ust. 1, nieprawdziwe, niekompletne lub nieaktualne dane osobowe lub przesłał te dane z naruszeniem przepisów niniejszej ustawy, jest obowiązany bez zbędnej zwłoki poinformować o tym odbiorcę oraz:

1) sprostować, uzupełnić lub uaktualnić te dane, a także przesłać odbiorcy dane właściwe, chyba że z uwagi na upływ czasu jest to oczywiście nieuzasadnione, albo
2) usunąć lub ograniczyć przetwarzanie tych danych, a także poinformować o tym odbiorcę w celu usunięcia lub ograniczenia przez odbiorcę przetwarzania tych danych.

4. Ograniczenie przetwarzania danych, o którym mowa w ust. 3 pkt 2, następuje, w przypadku gdy:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić, lub
2) dane osobowe muszą zostać zachowane do celów dowodowych.

5. Przepisów ust. 1–3 nie stosuje się, w przypadku gdy przesłanie lub udostępnienie danych osobowych odbiorcom, o których mowa w ust. 1, mogłoby stanowić zagrożenie praw i wolności człowieka i obywatela, a także w przypadkach, o których mowa w art. 25 ust. 1.

6. Jeżeli przepisy prawa, w tym prawa Unii, przewidują szczególne warunki przetwarzania, właściwy organ przesyłający jest zobowiązany do poinformowania odbiorcy takich danych osobowych o tych warunkach i obowiązku ich przestrzegania.

Rozdział 4

Prawa osoby, której dane dotyczą

Art. 22. 1. Administrator udostępnia informacje o:

1) nazwie, siedzibie i danych kontaktowych administratora;
2) w razie potrzeby danych kontaktowych inspektora ochrony danych;
3) celu, do których mają posłużyć dane osobowe;
4) prawie wniesienia do Prezesa Urzędu lub innego organu sprawującego nadzór na podstawie przepisów odrębnych skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych, oraz danych kontaktowych Prezesa Urzędu lub innego organu sprawującego nadzór;
5) prawie żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych, lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby.

2. Informacje, o których mowa w ust. 1, udostępnia się na stronie internetowej, w Biuletynie Informacji Publicznej na stronie podmiotowej lub w siedzibie właściwego organu lub urzędu.

3. Osobie, której dane dotyczą, w konkretnych przypadkach w celu umożliwienia wykonywania przysługujących jej praw, administrator przekazuje co najmniej następujące informacje:

1) podstawa prawna przetwarzania;

2) okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
3) odbiorcy lub kategorii odbiorców, którym dane osobowe zostały ujawnione, w szczególności odbiorcy w państwach trzecich lub organizacjach międzynarodowych.

4. Osobie, której dane dotyczą, przysługuje na jej wniosek prawo do uzyskania od administratora informacji, czy jej dane są przetwarzane, a w sytuacji ich przetwarzania prawo do informacji o:

1) celu i podstawie prawnej ich przetwarzania;
2) kategorii danych osobowych i danych, które są przetwarzane;
3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) okresie przechowywania danych osobowych lub, gdy nie jest to możliwe, o kryteriach służących określeniu tego okresu;
5) możliwości wniesienia wniosku do administratora o sprostowanie lub usunięcie danych osobowych, lub ograniczenie przetwarzania danych osobowych dotyczących tej osoby;
6) prawie wniesienia do Prezesa Urzędu lub innego organu sprawującego nadzór na podstawie przepisów odrębnych skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych, oraz danych kontaktowych Prezesa Urzędu lub innego organu sprawującego nadzór;
7) źródle pochodzenia danych.

Art. 23. 1. Osobie, której dane dotyczą, przysługuje, na jej wniosek, prawo dostępu do jej danych osobowych.

2. Uwzględniając wniosek o dostęp do danych osobowych, administrator udostępnia lub przekazuje wnioskodawcy ich kopię albo sporządzony w przystępnej formie wyciąg z tych danych.

3. Administrator informuje osobę, której dane dotyczą, o przyczynach odmowy lub ograniczenia dostępu oraz o możliwości wniesienia do Prezesa Urzędu skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych.

4. Administrator dokumentuje faktyczne lub prawne przyczyny odmowy lub ograniczenia dostępu do danych. Informację tę udostępnia się Prezesowi Urzędu na jego wniosek.

Art. 24. 1. Osoba, której dane dotyczą, może wystąpić z wnioskiem do administratora o niezwłoczne:

1) uzupełnienie, uaktualnienie lub sprostowanie danych osobowych – w przypadku gdy dane te są niekompletne, nieaktualne lub nieprawdziwe;
2) usunięcie danych osobowych – w przypadku gdy dane te zostały zebrane lub są przetwarzane z naruszeniem przepisów niniejszej ustawy.

2. Uwzględniając wniosek, o którym mowa w ust. 1, administrator bez zbędnej zwłoki odpowiednio uzupełnia, aktualizuje lub sprostowuje dane osobowe albo dokonuje ich usunięcia.

3. Jeżeli wniosek o sprostowanie lub uaktualnienie dotyczy danych, które znajdują się również w dokumencie zawierającym zeznanie, wypowiedź czy oświadczenie osoby fizycznej, a ustalono, że dane te są nieprawidłowe lub nieaktualne, administrator pozostawia je w postaci niezmienionej. Wniosek uwzględnia się tylko przez umieszczenie w zbiorze danych stosownej adnotacji.

4. W przypadku stwierdzenia z urzędu okoliczności, o której mowa w ust. 1 pkt 2, administrator dokonuje usunięcia danych osobowych.

5. Administrator informuje wnioskodawcę o sprostowaniu lub usunięciu danych lub o odmowie ich sprostowania lub usunięcia.

6. W przypadku odmowy sprostowania lub usunięcia danych osobowych administrator poucza osobę, której dane dotyczą, o możliwości wniesienia skargi, jeżeli jej dane osobowe są przetwarzane niezgodnie z prawem.

Art. 25. 1. Jeżeli:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić,
2) dane osobowe, które podlegają usunięciu, muszą zostać zachowane do celów dowodowych

– administrator jest obowiązany bez zbędnej zwłoki do czasowego ograniczenia przetwarzania kwestionowanych danych polegającego na nieudostępnianiu tych danych odbiorcom.

2. Administrator jest obowiązany poinformować bez zbędnej zwłoki właściwy organ, od którego pochodzą nieprawidłowe dane osobowe, o dokonanym sprostowaniu tych danych.

3. Administrator bez zbędnej zwłoki informuje odbiorców o dokonanym sprostowaniu lub usunięciu danych osobowych, lub ograniczeniu ich przetwarzania. Odbiorcy są

zobowiązani do uaktualnienia, sprostowania lub usunięcia danych osobowych, lub ograniczenia ich przetwarzania.

4. Przed zniesieniem ograniczenia przetwarzania kwestionowanych danych administrator informuje o tym osobę, której dane dotyczą.

5. Administrator informuje osobę, której dane dotyczą, o ograniczeniu przetwarzania danych osobowych, a także o możliwości wniesienia skargi, jeżeli jej dane osobowe są przetwarzane niezgodnie z prawem.

Art. 26. 1. Nie przekazuje się informacji, o których mowa w przepisach tego rozdziału, oraz nie udostępnia się danych osobowych, jeżeli mogłoby to powodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
4) zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
5) zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
6) istotne naruszenie dóbr osobistych innych osób.

2. Administrator może przekazać osobie, której dane dotyczą, informacje, o których mowa w ust. 1, w przypadku gdy ich ujawnienie byłoby niezbędne do ochrony życia lub zdrowia ludzkiego.

Art. 27. W odniesieniu do danych osobowych zgromadzonych w postępowaniach prowadzonych na podstawie ustaw, o których mowa w art. 3 pkt 1, prawa osób, których dane dotyczą, są wykonywane wyłącznie na podstawie i w zakresie przewidzianym przez przepisy regulujące te postępowania.

Art. 28. Wnioskodawca, składając wniosek na podstawie art. 22 ust. 4, art. 23 ust. 1 i art. 24 ust. 1 jest zobowiązany do podania co najmniej imienia i nazwiska oraz adresu korespondencyjnego. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby, która złożyła wniosek, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości tej osoby.

Art. 29. Administrator w przypadku, o którym mowa w art. 26 ust. 1, poucza osobę, której dane dotyczą, o możliwości wniesienia skargi do Prezesa Urzędu.

Art. 30. 1. Administrator podejmuje działania mające na celu ułatwienie osobie, której dane dotyczą, wykonywanie przysługujących jej praw, o których mowa w art. 15 i art. 22–25.

2. Administrator udziela informacji, o których mowa w art. 15, art. 22–25 i art. 45, osobie, której dane dotyczą, jasnym i prostym językiem, w takiej samej postaci, w jakiej wniesiono wniosek, chyba że udzielenie informacji w takiej postaci powodowałoby nadmierne trudności lub koszty lub przepis niniejszej ustawy stanowi inaczej.

3. Administrator, bez zbędnej zwłoki, informuje pisemnie w postaci papierowej lub elektronicznej lub za pośrednictwem środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650) osobę, której dane dotyczą, o działaniach podjętych w związku z jej wnioskiem lub, jeżeli to możliwe, udziela wnioskowanych informacji.

4. Komunikacja prowadzona przez administratora z osobą, której dane dotyczą, na podstawie art. 15, art. 22–25 i art. 45 jest wolna od opłat. Jeżeli żądania osoby, której dane dotyczą, są nieuzasadnione lub nadmierne, zwłaszcza ze względu na ich powtarzalność, administrator może:

1) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, lub
2) odmówić podjęcia działań w związku z żądaniem.

5. Opłatę, o której mowa w ust. 4 pkt 1, uiszcza się przed udzieleniem przez administratora informacji, prowadzeniem komunikacji lub podjęciem żądanych działań. Opłata pobierana przez administratora działającego w ramach jednostki budżetowej stanowi dochód budżetu państwa.

6. Administrator bez zbędnej zwłoki, lecz nie później niż w terminie do 14 dni od dnia złożenia wniosku, powiadomi wnioskodawcę o wysokości opłaty, o której mowa w ust. 4 pkt 1. Udzielenie informacji zgodnie z wnioskiem następuje po upływie 14 dni od dnia powiadomienia wnioskodawcy, chyba że wnioskodawca dokona w tym terminie zmiany wniosku co do zakresu żądanych danych, sposobu lub formy ich udostępnienia albo wycofa wniosek.

7. Obowiązek wykazania, że żądanie osoby, której dane dotyczą, jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na administratorze.

Rozdział 5

Administrator i podmiot przetwarzający

Oddział 1

Przepisy ogólne

Art. 31. 1. Administrator zapewnia, aby dane osobowe były:

1) przetwarzane zgodnie z prawem i rzetelnie oraz przy zastosowaniu niezbędnych środków technicznych i organizacyjnych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
2) przetwarzane w konkretnych i uzasadnionych celach;
3) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;
5) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;
6) 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 środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczone przed ich udostępnieniem osobom nieupoważnionym lub wejściem w posiadanie przez osobę nieuprawnioną.

2. Administrator podejmuje wszelkie działania, aby dane osobowe, które są nieprawidłowe, w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

3. Administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych i prawidłową realizację czynności w tym zakresie, o których mowa w ust. 1 i 2 i art. 13–21, oraz jest obowiązany do prowadzenia dokumentacji dotyczącej realizacji tych czynności. Dopuszcza się prowadzenie tej dokumentacji w postaci elektronicznej.

4. Administrator opracowuje i wdraża politykę ochrony danych, uwzględniając w niej sposób dokumentowania środków, o których mowa w ust. 1 pkt 1.

5. Administrator dokonuje bieżącego przeglądu środków, o których mowa w ust. 1 pkt 1, pod kątem potrzeby ich uaktualniania.

6. Inne podmioty przetwarzające dane osobowe w celach, o których mowa w art. 1 pkt 1, są zobowiązane do wykonywania obowiązków, o których mowa w ust. 1–5.

7. Administrator dokumentuje faktyczne lub prawne przyczyny odmowy przekazania informacji lub udostępnienia danych osobowych.

Art. 32. 1. Administrator, w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, stosuje odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, które zostały zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak aby spełnić wymogi niniejszej ustawy, chroniły prawa osób, których dane dotyczą, oraz uwzględniały stan wiedzy technicznej, koszt wdrożenia i charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia wynikające z przetwarzania.

2. Administrator stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia, aby domyślnie były przetwarzane wyłącznie te dane osobowe, które są niezbędne dla każdego konkretnego celu przetwarzania. Obowiązek ten ma zastosowanie do liczby zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te mają zapewnić, aby domyślnie dane osobowe nie były udostępniane bez interwencji osoby fizycznej nieokreślonej liczbie osób fizycznych lub innych podmiotów.

3. W polityce ochrony danych administrator określa odpowiednie środki techniczne oraz niezbędne zabezpieczenia stosowane przy przetwarzaniu danych osobowych w celu realizacji czynności, o których mowa w ust. 1 i 2.

Art. 33. 1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych osobowych w ramach jednego zbioru danych osobowych, stają się oni współadministratorami.

2. Współadministratorzy:

1) uzgadniają w drodze pisemnego porozumienia podział swoich obowiązków, w szczególności w zakresie:
   a) realizacji przez osobę, której dane dotyczą, przysługujących jej praw na mocy niniejszej ustawy,
   b) udzielania informacji, o których mowa w art. 22 ust. 4,

chyba że przepisy prawa, w tym prawa Unii Europejskiej, którym ci administratorzy podlegają, określają przypadające im obowiązki i ich zakres;

2) wyznaczają punkt kontaktowy dla osób, których dane dotyczą, w celu realizacji obowiązku, o którym mowa w pkt 1 lit. a.

Art. 34. 1. Administrator może w drodze umowy powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu.

2. Podmiot przetwarzający wdraża niezbędne środki techniczne i organizacyjne zapewniające przetwarzanie danych zgodnie z prawem i w sposób chroniący prawa osób, których dane dotyczą.

3. Umowa powierzenia, o której mowa w ust. 1, określa w szczególności:

1) przedmiot i okres jej obowiązywania;
2) charakter i cel przetwarzania;
3) rodzaj przetwarzanych danych osobowych;
4) kategorie osób, których dane dotyczą, o których mowa w art. 19;
5) prawa i obowiązki administratora;
6) obowiązki podmiotu przetwarzającego, o których mowa w ust. 5;
7) sposób prowadzenia przez administratora kontroli przetwarzania.

4. Umowę powierzenia, o której mowa w ust. 1, sporządza się w postaci pisemnej. Możliwe jest również sporządzenie umowy w postaci elektronicznej.

5. Podmiot przetwarzający jest zobowiązany:

1) przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie;
2) działać wyłącznie zgodnie z upoważnieniem administratora;
3) zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności, również w zakresie środków technicznych ich zabezpieczenia;
4) pomagać administratorowi w przestrzeganiu przepisów określających prawa osoby, której dane dotyczą;
5) po zakończeniu świadczenia usługi przetwarzania danych, w zależności od decyzji administratora:
   a) usunąć lub zwrócić administratorowi wszelkie dane osobowe oraz
   b) usunąć wszelkie istniejące kopie danych osobowych

   – chyba że przepisy prawa, w tym prawa Unii Europejskiej, wymagają przechowywania danych osobowych;

6) udostępniać administratorowi wszelkie informacje związane z weryfikacją prawidłowości realizacji umowy powierzenia, o której mowa w ust. 1;
7) przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, któremu powierzył przetwarzanie danych osobowych.

6. Podmiot przetwarzający może powierzyć przetwarzanie danych innemu podmiotowi przetwarzającemu każdorazowo wyłącznie na podstawie pisemnej umowy, w przypadku gdy umowa powierzenia przewiduje takie prawo, na warunkach i w zakresie przez nią określonym.

7. W przypadkach powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze, co nie wyłącza odpowiedzialności podmiotu przetwarzającego za przetwarzanie danych niezgodnie z ustawą lub umową powierzenia.

8. Jeżeli podmiot przetwarzający naruszy przepisy niniejszej ustawy w zakresie określenia celów lub sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Art. 35. 1. Administrator prowadzi wykaz kategorii czynności przetwarzania, za które odpowiada.

2. W wykazie, o którym mowa w ust. 1, zamieszcza się następujące informacje:

1) imię i nazwisko lub nazwę oraz dane kontaktowe:
   a) administratora,
   b) współadministratora – w przypadku, o którym mowa w art. 33 ust. 1,
   c) inspektora ochrony danych,
   d) podmiotu przetwarzającego – w przypadku, o którym mowa w art. 34 ust. 2 i 6;
2) cele przetwarzania;
3) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
4) opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych;
5) informacje o stosowaniu profilowania – w przypadku gdy zostało ono zastosowane;
6) kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
7) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;
8) planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe;

9) ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych, o których mowa w art. 39, jeżeli jest to możliwe.

3. Podmiot przetwarzający prowadzi wykaz kategorii czynności przetwarzania dokonywanych w imieniu administratora.

4. W wykazie, o którym mowa w ust. 3, zamieszcza się następujące informacje:

1) imię i nazwisko lub nazwę oraz dane kontaktowe:
   a) podmiotu przetwarzającego w przypadku, o którym mowa w art. 34 ust. 2 i 6,
   b) każdego administratora, w imieniu którego działa podmiot przetwarzający,
   c) inspektora ochrony danych;
2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
3) przypadki przekazania danych osobowych do państw trzecich lub organizacji międzynarodowej, w razie jednoznacznego polecenia administratora, łącznie z nazwą tego państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 39, w miarę możliwości.

5. Wykazy, o których mowa w ust. 1 i 3, prowadzi się w formie pisemnej, w postaci papierowej albo elektronicznej.

6. Administrator i podmiot przetwarzający udostępniają wykazy, o których mowa w ust. 1 i 3, Prezesowi Urzędu na jego żądanie.

Art. 36. 1. Operacje przetwarzania prowadzone w zautomatyzowanych systemach przetwarzania są ewidencjonowane.

2. Ewidencjonowaniu podlegają operacje przetwarzania, w szczególności:

1) zbieranie;
2) modyfikowanie;
3) przeglądanie;
4) ujawnianie wraz z przekazywaniem;
5) łączenie;
6) usuwanie.

3. Ewidencja jest prowadzona automatycznie, w sposób pozwalający ustalić zasadność operacji w oparciu o informacje wskazujące:

1) datę i godzinę operacji;
2) tożsamość osoby, która przeglądała lub ujawniła dane osobowe – w miarę możliwości;

3) tożsamość odbiorców danych osobowych – w miarę możliwości.

4. W ewidencji, która nie jest prowadzona w sposób automatyczny, dodatkowo zamieszcza się informację uzasadniającą zasadność operacji.

5. Ewidencje obejmujące czynności przetwarzania są przeznaczone wyłącznie:

1) do weryfikacji zgodności przetwarzania z prawem;
2) do monitorowania własnej działalności;
3) dla zapewnienia integralności i bezpieczeństwa danych osobowych;
4) na potrzeby postępowania karnego.

6. Administrator i podmiot przetwarzający udostępniają ewidencje obejmujące czynności przetwarzania Prezesowi Urzędu na jego żądanie.

Art. 37. 1. Jeżeli dany rodzaj przetwarzania danych osobowych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych, administrator – przed przetworzeniem danych osobowych – dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

2. Ocena, o której mowa w ust. 1, zawiera co najmniej:

1) ogólny opis planowanych operacji przetwarzania danych osobowych;
2) ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą;
3) środki planowane w celu rozwiązania takiego ryzyka;
4) zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazanie zgodności z niniejszą ustawą.

3. Realizację obowiązku, o którym mowa w ust. 1, administrator może powierzyć inspektorowi ochrony danych.

Art. 38. 1. Administrator lub podmiot przetwarzający, przed rozpoczęciem przetwarzania danych osobowych, które będzie częścią mającego powstać nowego zbioru danych, występują do Prezesa Urzędu z wnioskiem o konsultacje, jeżeli:

1) ocena, o której mowa w art. 37 ust. 1, wykaże, że przetwarzanie danych osobowych powodowałoby wysokie ryzyko naruszenia praw i wolności osób fizycznych w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka, lub
2) dany rodzaj przetwarzania danych osobowych stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą.

2. Prezes Urzędu może sporządzić wykaz operacji przetwarzania, które wymagają uprzednich konsultacji zgodnie z ust. 1. Wykaz ten Prezes Urzędu ogłasza w formie komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej Monitor Polski.

3. Administrator przedstawia Prezesowi Urzędu:

1) ocenę, o której mowa w art. 37 ust. 1, oraz
2) na żądanie Prezesa Urzędu – wszelkie inne informacje umożliwiające Prezesowi Urzędu ocenę zgodności przetwarzania z przepisami prawa, a w szczególności ocenę ryzyka w sferze ochrony danych osobowych osoby, której dane dotyczą, oraz powiązanych zabezpieczeń.

4. Jeżeli Prezes Urzędu uzna, że zamierzone przetwarzanie, o którym mowa w ust. 1 i 2, stanowiłoby naruszenie przepisów niniejszej ustawy, w szczególności jeżeli uzna, że administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko, w terminie do sześciu tygodni od dnia otrzymania wniosku o konsultacje, o którym mowa w ust. 1, przedstawia administratorowi lub podmiotowi przetwarzającemu pisemne zalecenia.

5. Z uwagi na złożony charakter sprawy termin, o którym mowa w ust. 4, może zostać przedłużony o miesiąc, o czym Prezes Urzędu informuje administratora lub podmiot przetwarzający w terminie miesiąca od otrzymania wniosku, o którym mowa w ust. 1, z podaniem uzasadnienia przyczyny wydłużenia tego terminu.

6. Realizację obowiązków, o których mowa w ust. 1–4, administrator może powierzyć inspektorowi ochrony danych.

Oddział 2

Zabezpieczenie danych osobowych

Art. 39. Administrator i podmiot przetwarzający stosują środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, które w szczególności mają na celu:

1) uniemożliwienie osobom nieuprawnionym dostępu do sprzętu używanego do przetwarzania (kontrola dostępu do sprzętu);
2) zapobiegnięcie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
3) zapobiegnięcie nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

4) zapobiegnięcie korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);
5) zapewnienie osobom, uprawnionym do korzystania z systemu zautomatyzowanego przetwarzania, dostępu wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);
6) umożliwienie zweryfikowania i ustalenia podmiotów, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione, za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);
7) umożliwienie następczej weryfikacji i ustalenia, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (kontrola wprowadzania danych);
8) zapobieżenie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);
9) zapewnienie przywrócenia zainstalowanych systemów w razie awarii (odzyskiwanie);
10) zapewnienie działania funkcji systemu, zgłaszania występujących w nich błędów (niezawodność) oraz odporności przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

Art. 40. Administrator i podmiot przetwarzający niszczą w sposób trwały niepodlegające archiwizacji informatyczne nośniki danych wykorzystywane do przetwarzania danych osobowych wycofane z eksploatacji przy użyciu odpowiednich narzędzi i środków technicznych. Nośniki wycofane z eksploatacji nie mogą być zbywane. Ze zniszczenia nośników sporządza się protokół, w którym uwzględnia się wskazanie sposobu ich zniszczenia.

Art. 41. 1. Do przetwarzania danych osobowych może być dopuszczona wyłącznie osoba zapewniająca bezpieczeństwo przetwarzanych danych osobowych oraz posiadająca upoważnienie do przetwarzania danych osobowych w ramach danej kategorii czynności przetwarzania, nadane przez administratora lub podmiot przetwarzający. Zatwierdzony przez administratora lub podmiot przetwarzający wniosek o nadanie uprawnień do dostępu do danych osobowych w ramach danej kategorii czynności przetwarzania uznaje się za nadanie takiego upoważnienia.

2. Wniosek o nadanie uprawnień dostępu do danych osobowych powinien zawierać w szczególności:

1) imię i nazwisko, stanowisko, miejsce zatrudnienia osoby, której wniosek dotyczy;
2) zakres i czasookres dostępu do danych osobowych;
3) rodzaj danych osobowych i sposób ich przetwarzania.

3. Do wniosku należy dołączyć oświadczenie osoby, której wniosek dotyczy, o zobowiązaniu się do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem.

4. Wniosek oraz oświadczenie, o których mowa w ust. 2 i 3, mogą być sporządzone w formie elektronicznej.

Art. 42. 1. Administrator lub podmiot przetwarzający prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera:

1) imię i nazwisko osoby upoważnionej;
2) datę udzielenia i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) identyfikator, jeżeli dane są przetwarzane w systemie teleinformatycznym.

2. Rolę ewidencji, o której mowa w ust. 1, może pełnić wykaz osób uprawnionych, prowadzony na podstawie zatwierdzonych przez administratora lub podmiot przetwarzający wniosków o nadanie uprawnień do dostępu do zbioru danych, o których mowa w art. 41.

Art. 43. Osoby, które zostały upoważnione do przetwarzania danych osobowych, są zobowiązane do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem, jak również do zachowania w tajemnicy udostępnionych danych osobowych oraz sposobów ich zabezpieczenia.

Art. 44. 1. W przypadku naruszenia ochrony danych osobowych, administrator, bez zbędnej zwłoki, nie później jednak niż w ciągu 72 godzin po stwierdzeniu naruszenia, zgłasza naruszenie Prezesowi Urzędu. Przepisu nie stosuje się, jeżeli nie wystąpiło ryzyko naruszenia praw i wolności osób fizycznych.

2. W przypadku niedotrzymania terminu, o którym mowa w ust. 1, administrator niezwłocznie zgłasza naruszenie oraz sporządza i przekazuje Prezesowi Urzędu uzasadnienie niedotrzymania tego terminu.

3. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je administratorowi, bez zbędnej zwłoki, nie później jednak niż w ciągu 48 godzin.

4. Zgłoszenie, o którym mowa w ust. 1 i 3, zawiera co najmniej następujące informacje:

1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wykazów danych osobowych, których dotyczy naruszenie;
2) imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, który może udzielić dodatkowych informacji;
3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
4) opis środków zastosowanych lub zaproponowanych przez administratora w celu usunięcia naruszenia ochrony danych osobowych, w tym zminimalizowania jego ewentualnych negatywnych skutków.

5. Jeżeli nie można przekazać informacji, o których mowa w ust. 4, w jednym zgłoszeniu, można je udzielać sukcesywnie bez zbędnej zwłoki.

6. Administrator dokumentuje dla celów kontrolnych przypadki naruszenia ochrony danych osobowych, o których mowa w ust. 1, podając okoliczności ich naruszenia, skutki oraz podjęte działania naprawcze, dołączając uwierzytelnioną przez siebie kopię zgłoszenia, o którym mowa w ust. 4.

7. W przypadku gdy naruszenie ochrony danych osobowych dotyczyło danych osobowych:

1) otrzymanych od administratora innego państwa członkowskiego Unii Europejskiej,
2) przesłanych do administratora innego państwa członkowskiego Unii Europejskiej

– informacje, o których mowa w ust. 4, przekazuje się bez zbędnej zwłoki administratorowi tego państwa członkowskiego Unii Europejskiej.

8. Prezes Urzędu może przeprowadzać kontrolę realizacji przez administratora obowiązków, o których mowa w ust. 1–7.

Art. 45. 1. W przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

2. Zawiadomienie, o którym mowa w ust. 1, zawiera w szczególności:

1) opis charakteru naruszenia ochrony danych osobowych;
2) informacje, o których mowa w art. 44 ust. 4 pkt 2–4.

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, jeżeli został spełniony jeden z poniższych warunków:

1) administrator zastosował odpowiednie techniczne i organizacyjne środki ochrony, w szczególności szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wskazanych w ust. 1;
3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku.

4. W przypadku, o którym mowa w ust. 3 pkt 3, administrator wydaje publiczny komunikat lub stosuje podobny środek zawierający elementy wskazane w ust. 2, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

5. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych, Prezes Urzędu, biorąc pod uwagę prawdopodobieństwo, że naruszenie ochrony danych osobowych spowoduje wysokie ryzyko, może:

1) zażądać wystosowania przez administratora zawiadomienia;
2) stwierdzić, że został spełniony jeden z warunków, o których mowa w ust. 3.

6. W przypadku, o którym mowa w art. 26 ust. 1, zawiadomienie, o którym mowa w ust. 1, można opóźnić, ograniczyć lub pominąć.

Oddział 3

Inspektor ochrony danych

Art. 46. 1. Administrator wyznacza inspektora ochrony danych.

2. Inspektorem ochrony danych może być osoba, która:

1) ukończyła studia wyższe;
2) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
3) posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;
4) nie była skazana prawomocnym wyrokiem, orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.

3. Administratorzy mogą wyznaczyć jednego inspektora ochrony danych dla kilku właściwych organów, uwzględniając ich strukturę organizacyjną i wielkość.

4. Inspektor ochrony danych podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem lub podmiotem przetwarzającym.

5. Administrator zapewnia odpowiednie i niezwłoczne włączenie inspektora ochrony danych we wszystkie sprawy dotyczące ochrony danych osobowych.

6. Administrator zawiadamia Prezesa Urzędu pisemnie, faxem, elektronicznie lub za pomocą elektronicznej platformy usług administracji publicznej ePUAP o wyznaczeniu inspektora ochrony danych w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

7. Administrator zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 6, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

8. Administrator udostępnia dane inspektora, o których mowa w ust. 6, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Art. 47. 1. Do zadań inspektora ochrony danych należy:

1) informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;
2) prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania;
3) monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami niniejszej ustawy oraz innymi przepisami dotyczącymi ochrony danych;
4) monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem;
5) współpraca z Prezesem Urzędu;
6) monitorowanie realizacji zaleceń, o których mowa w art. 38 ust. 4, oraz przedstawianie Prezesowi Urzędu stanu ich realizacji;
7) pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 38, oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach;

8) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37, oraz monitorowanie wykonania tych zaleceń;
9) sporządzanie i przekazywanie administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

2. Administrator wspiera inspektora ochrony danych w wypełnianiu zadań, o których mowa w ust. 1, zapewniając środki niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania oraz do podnoszenia wiedzy fachowej.

3. Administrator może powierzyć inspektorowi ochrony danych wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań inspektora ochrony danych oraz nie spowoduje to konfliktu interesów.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb i sposób realizacji zadań, o których mowa w ust. 1, uwzględniając konieczność zapewnienia prawidłowości realizacji zadań inspektora ochrony danych oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.

Rozdział 6

Współpraca z organami nadzorczymi w innych państwach Unii Europejskiej

Art. 48. 1. Prezes Urzędu udziela pomocy organom nadzorczym w innych państwach Unii Europejskiej na ich wniosek.

2. Wniosek o pomoc dotyczy w szczególności:

1) udzielenia informacji;
2) przeprowadzenia:
   a) konsultacji,
   b) kontroli,
   c) postępowań.

3. Prezes Urzędu podejmuje wszelkie działania, aby wniosek o pomoc zrealizować bez zbędnej zwłoki, nie później niż w terminie jednego miesiąca po otrzymaniu wniosku.

4. Prezes Urzędu może odmówić realizacji wniosku o pomoc wyłącznie w przypadku, gdy:

1) nie jest organem właściwym w zakresie przedmiotu tego wniosku;
2) wykonanie tego wniosku naruszyłoby przepis prawa.

5. Prezes Urzędu informuje organ nadzorczy w innych państwach Unii Europejskiej, od którego wniosek pochodzi, o odmowie realizacji wniosku oraz przedstawia powody odmowy.

6. Prezes Urzędu informuje organ nadzorczy w innych państwach Unii Europejskiej, od którego wniosek pochodzi, o wynikach lub, w razie potrzeby, o postępach lub działaniach podjętych w celu udzielenia odpowiedzi na ten wniosek.

7. Prezes Urzędu przekazuje informacje organowi nadzorczemu w innych państwach Unii Europejskiej, od którego wniosek pochodzi, pisemnie w formie papierowej lub elektronicznej w uzgodnionym formacie.

8. Prezes Urzędu nie pobiera od organu nadzorczego w innych państwach Unii Europejskiej, od którego wniosek pochodzi, opłaty za działania podejmowane w związku z jego realizacją.

9. W szczególnie uzasadnionych przypadkach Prezes Urzędu oraz organ nadzorczy w innych państwach Unii Europejskiej mogą uzgodnić zasady wzajemnej rekompensaty wydatków poniesionych w wyniku realizacji konkretnego wniosku o pomoc.

Art. 49. 1. Prezes Urzędu może występować do organów nadzorczych w innych państwach Unii Europejskiej z wnioskiem o pomoc, w szczególności o udzielnie informacji, przeprowadzenie konsultacji, kontroli lub postępowań.

2. Wniosek o pomoc zawiera wszelkie niezbędne informacje, w tym cel i uzasadnienie wniosku.

3. Prezes Urzędu może wykorzystywać informacje otrzymane od innego państwa członkowskiego w innych państwach Unii Europejskiej wyłącznie w celu określonym we wniosku o pomoc.

4. Prezes Urzędu może wnosić o uzyskanie od organu nadzorczego w innych państwach Unii Europejskiej informacji o wynikach lub, w razie potrzeby, o postępach lub działaniach podjętych w celu udzielenia odpowiedzi na ten wniosek.

Rozdział 7

Środki ochrony prawnej i odpowiedzialność prawna

Art. 50. 1. Osobie, której dane osobowe są przetwarzane niezgodnie z prawem, przysługuje prawo wniesienia skargi do Prezesa Urzędu w terminie 30 dni od powzięcia wiadomości o tym naruszeniu lub otrzymania informacji od administratora.

2. Prezes Urzędu udziela osobie, która wniosła skargę, pomocy prawnej na jej wniosek do czasu rozpatrzenia skargi przez Prezesa Urzędu.

3. Skargę można wnieść za pomocą formularza zamieszczonego na stronie internetowej Prezesa Urzędu, pisemnie, faxem, elektronicznie lub za pomocą elektronicznej platformy usług administracji publicznej ePUAP.

4. Prezes Urzędu informuje osobę, która wniosła skargę, o postępach w jej wyjaśnianiu, sposobie jej rozpatrzenia oraz możliwości złożenia skargi do sądu administracyjnego. Do rozpatrywania skarg stosuje się odpowiednio przepisy art. 225, art. 231 oraz art. 237–239 Kodeksu postępowania administracyjnego.

5. Prezes Urzędu nie przekazuje osobie, która wniosła skargę, informacji mogących wskazywać na przetwarzanie danych osobowych przez organy właściwe w sytuacjach, o których mowa w art. 26 ust. 1.

6. Prawo do zgłoszenia naruszenia przetwarzania danych osobowych przysługuje również osobom innym niż wymienione w ust. 1 w przypadku powzięcia przez nie wiarygodnej wiadomości o tym naruszeniu. Do rozpatrywania zgłoszeń stosuje się odpowiednio art. 225 Kodeksu postępowania administracyjnego.

7. Dane zgłaszającego naruszenie, o którym mowa w ust. 6, Prezes Urzędu zachowuje w poufności na uzasadniony wniosek zgłaszającego.

Art. 51. 1. Każdemu podmiotowi, wobec którego Prezes Urzędu wydał decyzję, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego.

2. Każdej osobie, której dane dotyczą, przysługuje prawo do wniesienia do sądu administracyjnego skargi, jeżeli Prezes Urzędu nie rozpatrzył skargi lub zgłoszenia wniesionego na mocy art. 50 lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy od dnia wpływu skargi, o postępach lub wyniku jej rozpatrzenia.

3. Do rozpatrywania skarg stosuje się przepisy ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2018 r. poz. 1302, 1467, 1544 i 1625), z tym że:

1) przekazanie akt i odpowiedzi na skargę następuje w terminie 30 dni od dnia otrzymania skargi;
2) skargę rozpatruje się w terminie 30 dni od dnia otrzymania akt wraz z odpowiedzią na skargę.

Art. 52. Osoba, której dane dotyczą, może umocować organizację społeczną o charakterze niezarobkowym, prowadzącą działalność statutową w interesie publicznym i działającą w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku

z ochroną ich danych osobowych – do wykonywania w jej imieniu praw, w tym wnoszenia środków zaskarżenia określonych w niniejszym rozdziale.

Art. 53. 1. Osobie, która poniosła szkodę lub doznała krzywdy w wyniku czynności naruszającej przepisy niniejszej ustawy, przysługuje od administratora odszkodowanie lub zadośćuczynienie.

2. W sprawach o roszczenia, o których mowa w ust. 1, stosuje się odpowiednio przepisy rozdziału 10 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

3. W sprawach o stwierdzenie niezgodności działania administratora z przepisami niniejszej ustawy, Prezes Urzędu może wytoczyć powództwo na rzecz i w imieniu osoby,

o której mowa w ust. 1, a także wstąpić do postępowania przed sądem w każdym jego stadium.

4. W przypadku przystąpienia Prezesa Urzędu do toczącego się postępowania przed sądem stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 1360, z późn. zm.[5)]) o interweniencie ubocznym.

Rozdział 8

Przepisy karne

Art. 54. 1. Kto przetwarza dane osobowe, o których mowa w przepisach o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, 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 wrażliwych, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Art. 55. Kto udaremnia lub istotnie utrudnia kontrolującemu przeprowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat dwóch.

---

5) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 1467, 1499, 1544, 1629, 1637 i 1693.

Rozdział 9

Przepisy zmieniające

Art. 56. W ustawie z dnia 26 marca 1982 r. o Trybunale Stanu (Dz. U. z 2016 r. poz. 2050) po art. 20e dodaje się art. 20f i art. 20g w brzmieniu:

„Art. 20f. Trybunał Stanu jest administratorem danych osobowych przetwarzanych w ramach prowadzonych przez niego postępowań.

Art. 20g. 1. Nadzór nad przetwarzaniem danych osobowych przez Trybunał Stanu w ramach prowadzonych przez niego postępowań wykonuje Krajowa Rada Sądownictwa.

2. Do nadzoru, o którym mowa w ust. 1, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2018 r. poz. 23, z późn. zm.[6)]) stosuje się odpowiednio.”.

Art. 57. W ustawie z dnia 18 kwietnia 1985 r. o rybactwie śródlądowym (Dz. U. z 2018 r. poz. 1476) wprowadza się następujące zmiany:

1) po art. 22 dodaje się art. 22a i art. 22b w brzmieniu:

„Art. 22a. 1. Państwowa Straż Rybacka w celu realizacji ustawowych zadań jest uprawniona do przetwarzania informacji, w tym danych osobowych, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzania danych genetycznych danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej.

2. Państwowa Straż Rybacka może przetwarzać dane osobowe bez wiedzy i zgody osoby, której dane dotyczą, w celu realizacji swoich ustawowych zadań.

3. Administratorem danych osobowych przetwarzanych w celach, o których mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest komendant wojewódzki Państwowej Straży Rybackiej.

4. Państwowa Straż Rybacka w celu realizacji zadań ustawowych, w szczególności dotyczących wykrywania i zwalczania przestępstw lub wykroczeń oraz identyfikacji

---

6) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 3, 5, 106, 138, 771, 848, 1000, 1045, 1443, 1544 i 1669.

osób w ramach wykonywanych czynności, jest uprawniona do uzyskiwania informacji, w tym danych osobowych, od innych służb, instytucji państwowych oraz organów władzy publicznej, w szczególności:

1) gromadzonych w zbiorach danych lub rejestrach prowadzonych przez te podmioty;
2) uzyskanych w wyniku wykonywania swoich zadań ustawowych przez te podmioty.

5. W przypadku, o którym mowa w ust. 4, służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia Państwowej Straży Rybackiej informacji, w tym danych osobowych.

6. Służby, instytucje państwowe oraz organy władzy publicznej administrujące zbiorami danych lub rejestrami, o których mowa w ust. 4 pkt 1, mogą wyrazić zgodę na udostępnianie za pomocą urządzeń telekomunikacyjnych (teletransmisji) informacji zgromadzonych w tych zbiorach lub rejestrach jednostkom organizacyjnym Państwowej Straży Rybackiej bez konieczności składania pisemnych wniosków w postaci papierowej lub elektronicznej, jeżeli jednostki te spełniają łącznie następujące warunki:

1) posiadają urządzenia umożliwiające odnotowanie w systemie kto, kiedy, w jakim celu oraz jakie dane uzyskał;
2) posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie informacji, w tym danych osobowych, niezgodnie z celem ich uzyskania;
3) jest to uzasadnione specyfiką lub zakresem wykonywania zadań albo prowadzonej działalności.

Art. 22b. 1. Państwowa Straż Rybacka jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w Państwowej Straży Rybackiej, przenoszenia do służby w Państwowej Straży Rybackiej oraz w zakresie wynikającym z przebiegu stosunku służbowego funkcjonariuszy Państwowej Straży Rybackiej, także po jego ustaniu, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia (UE) 2016/679, z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 tego rozporządzenia w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie

pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności.”;

2) po art. 24 dodaje się art. 24a w brzmieniu:

„Art. 24a. 1. Społeczna Straż Rybacka w celu realizacji ustawowych zadań jest uprawniona do przetwarzania informacji, w tym danych osobowych, z wyłączeniem danych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej.

2. Społeczna Straż Rybacka może przetwarzać dane osobowe bez wiedzy i zgody osoby, której dane dotyczą, w celu realizacji swoich ustawowych zadań.

3. Administratorem danych osobowych przetwarzanych w celach, o których mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości jest komendant właściwej jednostki Społecznej Straży Rybackiej.”.

Art. 58. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.[7)]) wprowadza się następujące zmiany:

1) w art. 1 w ust. 1 pkt 8 otrzymuje brzmienie:

„8) przetwarzanie informacji kryminalnych, w tym danych osobowych;”;

2) w art. 14:

a) w ust. 1 w pkt 1 po wyrazie „przestępstw” dodaje się przecinek i wyrazy „przestępstw skarbowych”,

b) w ust. 4 wyrazy „ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)” zastępuje się wyrazami „ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …)”;

[7)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544 i 1669.

3) w art. 15:

a) w ust. 1:

– w pkt 3a w lit. c średnik zastępuje się przecinkiem i dodaje się lit. d w brzmieniu:

„d) w celu identyfikacji lub wykrywania sprawców przestępstw – na zasadach określonych w niniejszej ustawie;”,

– po pkt 5a dodaje się pkt 5b w brzmieniu:

„5b) obserwowania i rejestrowania przy użyciu środków technicznych obrazu lub dźwięku w trakcie interwencji w miejscach innych niż publiczne, podczas prowadzenia działań kontrterrorystycznych oraz wspierania działań jednostek organizacyjnych Policji przez służbę kontrterrorystyczną w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił i środków oraz specjalistycznej taktyki działań, a także w policyjnych środkach transportu;”,

b) po ust. 7b dodaje się ust. 7c w brzmieniu:

„7c. Użyte w pkt 5b określenie interwencja oznacza włączenie się policjanta lub policjantów w tok zdarzenia mogącego naruszać normy prawne i podjęcie działań zmierzających do ustalenia charakteru, rodzaju i okoliczności powstałego zdarzenia oraz przedsięwzięć ukierunkowanych na przywrócenie naruszonego porządku prawnego.”,

c) ust. 8 otrzymuje brzmienie:

„8. Rada Ministrów określi, w drodze rozporządzenia, sposób postępowania przy wykonywaniu uprawnień, o których mowa w ust. 1 pkt 1, 2a, 3, pkt 3a lit. b–d, pkt 3b i 5–7, oraz wzory dokumentów stosowanych w tych sprawach, mając na względzie zapewnienie skuteczności działań podejmowanych przez Policję oraz poszanowanie praw osób, wobec których działania te są podejmowane.”;

4) po art. 15a dodaje się art. 15b i art. 15c w brzmieniu:

„Art. 15b.1. Informacje uzyskane podczas realizacji czynności, o których mowa w art. 15 ust. 1 pkt 5a i 5b, w tym dane osobowe niezawierające dowodów pozwalających na wszczęcie postępowania karnego albo postępowania w sprawach o wykroczenia, postępowania dyscyplinarnego lub mogących być wykorzystanymi

w postępowaniu w ramach czynności wyjaśniających albo dowodów mających znaczenie dla toczących się takich postępowań, Policja przechowuje przez okres co najmniej 30 dni, nie dłużej jednak niż 60 dni od dnia zarejestrowania, a następnie je niszczy.

2. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób przechowywania, odtwarzania i kopiowania zapisów, sposób i tryb udostępniania zapisu obrazu i dźwięku uprawnionym podmiotom, mając na uwadze konieczność właściwego zabezpieczenia utrwalonego obrazu i dźwięku przed utratą, zniekształceniem lub nieuprawnionym ujawnieniem oraz zapewnienie ochrony praw osób, których wizerunek został utrwalony.

Art. 15c. W przypadkach, o których mowa w art. 15 ust. 1 pkt 5b, z wyłączeniem działań kontrterrorystycznych oraz wspierania działań jednostek organizacyjnych Policji przez służbę kontrterrorystyczną w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił i środków oraz specjalistycznej taktyki działań, funkcjonariusz Policji w miarę możliwości uprzedza osobę, wobec której podejmuje czynności, o rejestrowaniu obrazu lub dźwięku.”;

5) w art. 20:

a) ust. 1 otrzymuje brzmienie:

„1. W celu realizacji zadań ustawowych Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, z zachowaniem ograniczeń wynikających z art. 19.”,

b) po ust. 1 dodaje się ust. 1a–1o w brzmieniu:

„1a. Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może dotyczyć danych osobowych, o których mowa w art. 14 ust. 1 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przy czym dane dotyczące wyników analizy kwasu deoksyrybonukleinowego (DNA) obejmują informacje wyłącznie o niekodującej części DNA.

1b. Uzyskiwanie informacji, w tym danych osobowych, może odbywać się z wykorzystaniem środków technicznych.

1c. Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do realizacji zadań ustawowych lub wykonywania uprawnień związanych z prowadzeniem postępowań

administracyjnych, realizacją czynności administracyjno-porządkowych oraz innych czynności, do przeprowadzania których funkcjonariusze Policji są uprawnieni na podstawie ustaw, w celach innych niż określone w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 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 osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[8)]), zwanego dalej „rozporządzeniem (UE) 2016/679", z wyłączeniem danych dotyczących kodu genetycznego.

1d. Policja w zakresie swojej właściwości przetwarza informacje, w tym dane osobowe, uzyskane ze zbiorów danych prowadzonych przez inne służby, instytucje państwowe oraz organy władzy publicznej. Przetwarzanie informacji, w tym danych osobowych, przez Policję może mieć charakter niejawny, odbywać się bez zgody i wiedzy której dotyczą, oraz z wykorzystaniem środków technicznych. Służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia Policji informacji, w tym danych osobowych. W szczególności Policja jest uprawniona do uzyskiwania informacji, w tym danych osobowych:

1) gromadzonych w administrowanych przez nich zbiorach danych lub rejestrach;
2) uzyskanych przez te służby lub organy w wyniku wykonywania czynności operacyjno-rozpoznawczych, w tym prowadzonej kontroli operacyjnej.

---

8) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

1e. Podmioty, o których mowa w ust. 1d, mogą wyrazić pisemną zgodę na udostępnianie danych zgromadzonych w zbiorach danych jednostkom organizacyjnym Policji w drodze teletransmisji, bez konieczności składania wniosku pisemnie w postaci papierowej lub elektronicznej, jeżeli jednostki te spełniają łącznie następujące warunki:

1) posiadają urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał;
2) posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania;
3) jest to uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności.

1f. Komendant Główny Policji, Komendant CBŚP, Komendant BSWP, dyrektor Centralnego Laboratorium Kryminalistycznego Policji, komendanci wojewódzcy (Stołeczny) Policji, komendanci powiatowi (miejscy i rejonowi) Policji, Komendant-Rektor Wyższej Szkoły Policji w Szczytnie oraz komendanci szkół policyjnych są administratorami danych osobowych w stosunku do zbiorów danych osobowych utworzonych przez nich w celu realizacji zadań ustawowych.

1g. Kierownicy jednostek organizacyjnych Policji, o których mowa w ust. 1f, mogą tworzyć lub likwidować w drodze decyzji systemy, zbiory danych lub zestawy zbiorów danych, inne niż określone w niniejszej ustawie, w których przetwarza się informacje, w tym dane osobowe, w celu realizacji przez Policję zadań ustawowych.

1h. W przypadku likwidowania systemów, zbiorów danych lub zestawów zbiorów informacji, w tym danych osobowych, dokonuje tego komisja wyznaczana przez kierowników jednostek organizacyjnych Policji, o których mowa w ust. 1f, z czego sporządza się protokół.

1i. Kierownicy jednostek organizacyjnych Policji, o których mowa w ust. 1f, prowadzą rejestr systemów, zbiorów danych lub zestawów zbiorów danych, w których przetwarza się informacje, w tym dane osobowe.

1j. Przetwarzanie danych osobowych przez Policję w celach, o których mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na

podstawie ustawy, prawa Unii Europejskiej oraz postanowień umów międzynarodowych.

1k. W przypadku podejrzanych Policja pobiera wymazy ze śluzówki policzków oraz dane osobowe, o których mowa w art. 21a ust. 2 pkt 2 lit. b–h i art. 21h ust. 2 pkt 2 i 3, w celach, o których mowa w art. 15 ust. 1 pkt 3a lit. d.

1l. Policja pobiera odciski linii papilarnych lub wymazy ze śluzówki policzków od funkcjonariuszy i pracowników Policji wykonujących służbowe czynności związane z ujawnianiem, zabezpieczaniem lub badaniem śladów związanych z podejrzeniem popełnienia czynu zabronionego w celach wyeliminowania pozostawionych przez nich śladów.

1m. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb pobierania odcisków linii papilarnych lub wymazów ze śluzówki policzków od funkcjonariuszy i pracowników Policji oraz sposób przeprowadzania i dokumentowania czynności związanych z ich pobieraniem, a także rodzaje służb policyjnych uprawnionych do korzystania ze zbiorów danych zawierających odciski linii papilarnych lub wymazy ze śluzówki policzków od funkcjonariuszy i pracowników Policji oraz sposób zabezpieczenia tych zbiorów uniemożliwiający identyfikację funkcjonariusza lub pracownika Policji, których dane dotyczą, przez osobę nieupoważnioną, uwzględniając konieczność wyeliminowania pozostawionych przez nich śladów.

1n. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wzory dokumentów obowiązujących przy przetwarzaniu danych, uwzględniając potrzebę ochrony danych przed nieuprawnionym dostępem i przesłanki zaniechania zbierania określonych rodzajów informacji, a w przypadku wymiany informacji – uwzględniając konieczność dostosowania się do wymogów określonych przez organy innych państw, zobowiązania międzynarodowe Rzeczypospolitej Polskiej lub przez Międzynarodową Organizację Policji Kryminalnej – Interpol.

1o. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wzory kart daktyloskopijnych, na których dane daktyloskopijne są pobierane przez upoważnione podmioty i przekazywane Komendantowi Głównemu Policji w celu przetwarzania w zbiorach danych daktyloskopijnych, oraz tryb i sposób ich przekazywania Komendantowi Głównemu Policji przez

zobowiązane do tego służby, instytucje państwowe oraz organy władzy publicznej – uwzględniając charakter realizowanych zadań i celów przeznaczenia danej karty daktyloskopijnej.”,

c) uchyla się ust. 2a,

d) ust. 2aa i 2ab otrzymują brzmienie:

„2aa. W celu realizacji zadań ustawowych Policja jest uprawniona do wymiany informacji, w tym danych osobowych, z organami ścigania państw członkowskich Unii Europejskiej i innych państw, agencjami Unii Europejskiej zajmującymi się zapobieganiem i zwalczaniem przestępczości, Międzynarodową Organizacją Policji Kryminalnej – Interpol oraz innymi organizacjami międzynarodowymi na zasadach i warunkach określonych w przepisach odrębnych, prawie Unii Europejskiej oraz umowach międzynarodowych.

2ab. Policja jest uprawniona do przetwarzania i wymiany informacji, w tym danych osobowych osób ubiegających się o przyjęcie do pracy w agencjach Unii Europejskiej zajmujących się zapobieganiem lub zwalczaniem czynów zabronionych, międzynarodowych organach sądowniczych, międzynarodowych organach ścigania oraz w Międzynarodowej Organizacji Policji Kryminalnej – Interpol, za zgodą tych osób. Policja, przekazując wyniki przetwarzania, zastrzega, że nie udostępnia się ich osobie, której dane osobowe dotyczą.”,

e) uchyla się ust. 2ac,

f) w ust. 2b pkt 1 otrzymuje brzmienie:

„1) dane osobowe, o których mowa w art. 14 ust. 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z tym że dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA;”,

g) ust. 2c otrzymuje brzmienie:

„2c. Danych osobowych, o których mowa w art. 14 ust. 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej.”,

h) w ust. 4 dodaje się zdanie trzecie w brzmieniu: „Informacje i dane udostępnia się także organom ścigania państw członkowskich Unii Europejskiej, agencjom Unii Europejskiej zajmującym się zapobieganiem i zwalczaniem przestępczości oraz

Międzynarodowej Organizacji Policji Kryminalnej – Interpol, jeżeli następuje to w celu ścigania karnego.”,

i) w ust. 7 po wyrazach „rozpatrzeniu wniosku” dodaje się przecinek oraz wyrazy „o którym mowa w ust. 5,”,

j) uchyla się ust. 15–19;

6) w art. 20a po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Ochrona, o której mowa w ust. 1, może być realizowana przez obserwowanie i rejestrowanie wykonywanych zadań służbowych, obiektów Policji i policyjnych środków transportu.”;

7) w art. 20c wprowadza się następujące zmiany:

a) w ust. 1 po wyrazie „przestępstw” dodaje się przecinek i wyrazy „przestępstw skarbowych”,

b) po ust. 6 dodaje się ust. 6a w brzmieniu:

„6a. Komendant Główny Policji, Komendant CBŚP, Komendant BSWP albo komendant wojewódzki (Stołeczny) Policji może upoważnić swojego zastępcę do realizacji czynności, o których mowa w ust. 6.”,

c) dodaje się ust. 8 w brzmieniu:

„8. Dane, o których mowa w ust. 1, pobiera się i udostępnia się także organom ścigania państw członkowskich Unii Europejskiej i innych państw, agencjom Unii Europejskiej zajmującym się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol na ich wniosek, jeżeli następuje to w celu ścigania karnego albo w celu ratowania życia lub zdrowia ludzkiego.”;

8) w art. 20cb:

a) w ust. 1 po wyrazie „przestępstw” dodaje się przecinek i wyrazy „przestępstw skarbowych”,

b) ust. 2 otrzymuje brzmienie:

„2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, przepisy art. 20c ust. 2–8 stosuje się.”;

9) w art. 20da w ust. 1 wyrazy „przepisy art. 20c ust. 2–7 stosuje się” zastępuje się wyrazami „przepisy art. 20c ust. 2–8 stosuje się”;

10) w art. 20e ust. 1 otrzymuje brzmienie:

„1. Komendant Główny Policji prowadzi System Wspomagania Dowodzenia Policji, zwany dalej „SWD Policji”, będący systemem teleinformatycznym wspierającym:

1) wykonywanie zadań ustawowych przez jednostki organizacyjne Policji;
2) obsługę zgłoszeń alarmowych, o których mowa w ustawie z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz. U. z 2018 r. poz. 867 i 1115).”;

11) po art. 20e dodaje się art. 20f w brzmieniu:

„Art. 20f. 1. W związku z obsługą zadań, o których mowa w art. 20e ust. 1 pkt 1, Komendant Główny Policji przetwarza w SWD Policji informacje, w tym dane osobowe osób, których dane uzyskano w związku z realizacją zadań, o których mowa w art. 1 ust. 2 i 3, i w tym zakresie jest administratorem w rozumieniu przepisów o ochronie danych osobowych.

2. W związku z obsługą zgłoszeń alarmowych, o których mowa w art. 20e ust. 1 pkt 2, Komendant Główny Policji przetwarza w SWD Policji informacje, w tym dane osobowe osób określonych w ustawie z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego, i w tym zakresie jest administratorem w rozumieniu przepisów o ochronie danych osobowych.

3. Komendant Główny Policji przetwarza w SWD Policji informacje, w tym dane osobowe, w celu:

1) ewidencjonowania i dokumentowania przyjmowanych zgłoszeń o zdarzeniach oraz podjętych interwencjach;
2) zapewnienia właściwej reakcji Policji na zdarzenie;
3) współdziałania Policji z centrami powiadamiania ratunkowego oraz innymi służbami ratowniczymi;
4) zabezpieczania danych o źródłach dowodowych oraz prowadzenia analizy zagrożenia.

4. Informacje, w tym dane osobowe, przetwarzane w SWD Policji usuwa się automatycznie po upływie 5 lat od ich rejestracji.”;

12) art. 21a–21e otrzymują brzmienie:

„Art. 21a. 1. Komendant Główny Policji prowadzi zbiór danych zawierający informacje o wynikach analizy kwasu deoksyrybonukleinowego (DNA), zwany dalej

„zbiorem danych DNA”, którego jest administratorem w rozumieniu ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

2. W zbiorze danych DNA przetwarza się:

1) informacje, w tym dane osobowe, o których mowa w ust. 1, w odniesieniu do:
   a) osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego,
   b) nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego,
   c) osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396 oraz z 2016 r. poz. 2205),
   d) osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452, 650 i 730),
   e) oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego,
   f) osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość,
   g) zwłok ludzkich o nieustalonej tożsamości,
   h) śladów nieznanych sprawców przestępstw,
   i) osób zaginionych,
   j) osób, o których mowa w art. 15 ust. 1 pkt 3a lit. c,
   k) osób, o których mowa w art. 20 ust. 1l;
2) informacje, w tym dane osobowe osób, o których mowa w pkt 1 lit. a–e oraz i–k, obejmują:
   a) wyniki analizy kwasu deoksyrybonukleinowego (DNA),
   b) imiona, nazwiska lub pseudonimy,
   c) imiona i nazwiska rodowe rodziców tych osób,
   d) datę i miejsce urodzenia,
   e) adres zamieszkania,
   f) numer PESEL,
   g) obywatelstwo i płeć,
   h) oznaczenie i cechy dokumentu tożsamości.

3. W ramach zbioru danych DNA gromadzi się próbki pobrane od osoby albo ze zwłok ludzkich, w celu przeprowadzenia analizy kwasu deoksyrybonukleinowego (DNA), w postaci wymazów ze śluzówki policzków, krwi, cebulek włosów lub wydzielin, a w odniesieniu do zwłok ludzkich materiał biologiczny w postaci próbek z tkanek, zwane dalej „próbkami biologicznymi”.

Art. 21b. 1. Informacje, w tym dane osobowe, o których mowa w art. 21a ust. 2 pkt 1 lit. a–j, wprowadza się do zbioru danych DNA na podstawie zarządzenia:

1) prowadzącego postępowanie przygotowawcze lub sądu – w przypadku analizy kwasu deoksyrybonukleinowego (DNA) przeprowadzonej w związku z:
   a) postępowaniem karnym,
   b) postępowaniem w sprawach nieletnich,
   c) postępowaniem określonym w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób,
   d) postępowaniem wobec osób wymienionych w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych,
   e) postępowaniem wobec osób skazanych;
2) prowadzącego czynności – w przypadku osób o nieustalonej tożsamości, osób usiłujących ukryć swoją tożsamość, zwłok ludzkich o nieustalonej tożsamości, osób zaginionych oraz osób, o których mowa w art. 15 ust. 1 pkt 3a lit. c.

2. Informacje, w tym dane osobowe, o których mowa w art. 21a ust. 2 pkt 1 lit. k, wprowadza się do zbioru danych DNA na podstawie wniosku właściwego miejscowo organu Policji, przed podjęciem przez policjantów i pracowników Policji pierwszych czynności służbowych związanych z ujawnianiem, zabezpieczaniem lub badaniem śladów związanych z podejrzeniem popełnienia czynu zabronionego.

Art. 21c. Informacje, w tym dane osobowe, przetwarzane w zbiorze danych DNA udostępnia się bezpłatnie organom prowadzącym postępowanie karne, postępowanie w sprawach nieletnich lub prowadzącym czynności wykrywcze lub identyfikacyjne.

Art. 21d. 1. Informacje, w tym dane osobowe, o których mowa w art. 20 ust. 1l, są przetwarzane w zbiorze danych DNA w celu prowadzenia czynności wykrywczych lub identyfikacyjnych.

2. Informacje, w tym dane osobowe, o których mowa w art. 21a ust. 2 pkt 1 lit. a–j, są przetwarzane w zbiorze danych DNA w celu prowadzenia czynności wykrywczych i eliminacyjnych.

Art. 21e. 1. W weryfikacji, o której mowa w art. 16 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku zapobieganiem i zwalczaniem przestępczości, uczestniczą jednostki organizacyjne Policji, służby, instytucje państwowe lub organy władzy publicznej, które przekazały informacje, w tym dane osobowe, do zbioru danych DNA.

2. Informacje, w tym dane osobowe, usuwa się ze zbioru danych DNA, w przypadku gdy:

1) zostało umorzone postępowanie z uwagi na to, że:
   a) czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia,
   b) zdarzenie lub okoliczność, w związku z którymi wprowadzono dane osobowe do zbioru danych, nie ma znamion czynu zabronionego;
2) osoba, której dane dotyczą:
   a) została uniewinniona prawomocnym wyrokiem sądu,
   b) ukończyła 100. rok życia,
   c) zmarła;
3) tożsamość zwłok ludzkich została ustalona;
4) utracą swoją przydatność eliminacyjną, jednakże nie dłużej niż po upływie 5 lat od dnia ustania stosunku służbowego lub pracy – w przypadku osób, o których mowa w art. 20 ust. 1l.

3. Informacje, w tym dane osobowe osób, o których mowa w art. 21a ust. 2 pkt 1 lit. h, usuwa się ze zbioru danych DNA, po upływie okresu przedawnienia karalności przestępstwa, na wniosek organu prowadzącego postępowanie karne.

4. Informacje, w tym dane osobowe osób, o których mowa w art. 21a ust. 2 pkt 1 lit. i oraz j, usuwa się ze zbioru danych DNA, w przypadku odnalezienia lub ustalenia miejsca pobytu osoby zaginionej lub po upływie 55 lat od dnia rozpoczęcia ich przetwarzania w zbiorze danych DNA. Informacje te, w tym dane osobowe, usuwa się na wniosek jednostki organizacyjnej, służby, instytucji państwowej lub organu władzy publicznej prowadzącej poszukiwanie lub osoby zaginionej.

5. Usunięcia informacji, w tym danych osobowych osób, o których mowa w art. 21a ust. 2 pkt 1 lit. a–g oraz i–k, ze zbioru danych DNA oraz zniszczenia próbek biologicznych dokonuje komisja powołana przez Komendanta Głównego Policji, sporządzając z tych czynności protokół.”;

13) uchyla się art. 21f i art. 21g;

14) art. 21h–21n otrzymują brzmienie:

„Art. 21h. 1. Komendant Główny Policji prowadzi następujące zbiory danych daktyloskopijnych, których jest administratorem w rozumieniu przepisów o ochronie danych osobowych:

1) Centralną Registraturę Daktyloskopijną, w której są gromadzone karty daktyloskopijne i chejroskopijne zawierające odciski linii papilarnych osób,
2) zbiór automatycznie przetwarzający dane daktyloskopijne, w którym są przetwarzane informacje, w tym dane osobowe, o odciskach linii papilarnych osób, niezidentyfikowanych śladach linii papilarnych z miejsc przestępstw oraz śladach linii papilarnych, które mogą pochodzić od osób zaginionych

– zwane dalej łącznie „zbiorami danych daktyloskopijnych”.

2. W zbiorach danych daktyloskopijnych są przetwarzane:

1) informacje, w tym dane osobowe, dotyczące:
   a) osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego,
   b) nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego,
   c) osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób,
   d) osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych,
   e) oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego,
   f) osób poszukiwanych,
   g) cudzoziemców, od których zostały pobrane odciski linii papilarnych w sytuacjach, o których mowa w art. 35 ust. 2, art. 324 pkt 1 i art. 394 ust. 3

ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach lub art. 30 ust. 1 pkt 3, art. 92 ust. 1 i art. 114 ust. 1 ustawy z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej, lub art. 73a ustawy z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin (Dz. U. z 2017 r. poz. 900 oraz z 2018 r. poz. 650),

h) śladów linii papilarnych, które mogą pochodzić od osób zaginionych,

i) niezidentyfikowanych śladów linii papilarnych z miejsc przestępstw,

j) osób, o których mowa w art. 20 ust. 1l;

2) informacje, w tym dane osobowe, przetwarzane w zbiorze danych, o którym mowa w ust. 1 pkt 1, obejmują:

a) imiona, nazwiska lub pseudonimy,

b) imiona i nazwiska rodowe rodziców tych osób,

c) datę i miejsce urodzenia,

d) oznaczenie i cechy identyfikacyjne dokumentu tożsamości,

e) adres zamieszkania,

f) numer PESEL,

g) obywatelstwo i płeć,

h) oznaczenie i numer sprawy,

i) miejsce i powód daktyloskopowania,

j) odciski linii papilarnych palców i dłoni;

3) informacje, w tym dane osobowe, przetwarzane w zbiorze danych, o którym mowa w ust. 1 pkt 2, obejmujące:

a) obrazy odcisków linii papilarnych,

b) rok urodzenia,

c) płeć,

d) rodzaj rejestracji,

e) datę wprowadzenia,

f) jednostkę organizacyjną wprowadzającą;

4) informacje, w tym dane osobowe, dotyczące niezidentyfikowanych śladów linii papilarnych z miejsc przestępstw obejmujące:

a) obrazy śladów linii papilarnych,

b) datę i miejsce zabezpieczenia,

c) kategorię przestępstwa,

d) jednostkę organizacyjną wprowadzającą,

e) oznaczenie i numer sprawy;

5) informacje, w tym dane osobowe, dotyczące śladów linii papilarnych, które mogą pochodzić od osób zaginionych, obejmujące:

a) obrazy śladów linii papilarnych,

b) datę i miejsce zabezpieczenia,

c) kategorię zdarzenia,

d) jednostkę organizacyjną wprowadzającą,

e) oznaczenie i numer sprawy.

3. W zbiorach danych daktyloskopijnych przetwarza się, z wyłączeniem przechowywania, informacje, w tym dane osobowe, dotyczące osób o nieustalonej tożsamości lub usiłujących ukryć swoją tożsamość oraz zwłok ludzkich o nieustalonej tożsamości, obejmujące:

1) obrazy odcisków linii papilarnych;

2) płeć;

3) oznaczenie i numer sprawy.

Art. 21i. Informacje, w tym dane osobowe, wprowadza się do zbiorów danych daktyloskopijnych na podstawie wniosku organu prowadzącego postępowanie lub poszukiwanie osoby zaginionej.

Art. 21j. Informacje, w tym dane osobowe, przetwarzane w zbiorach danych daktyloskopijnych oraz uzyskane w wyniku ich przetwarzania są udzielane bezpłatnie organom prowadzącym:

1) postępowanie karne;

2) postępowanie w sprawach nieletnich;

3) czynności wykrywcze lub identyfikacyjne;

4) czynności związane z wprowadzaniem danych daktyloskopijnych do innych zbiorów danych na podstawie odrębnych przepisów.

Art. 21k. 1. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. a–h, są przechowywane w zbiorach danych daktyloskopijnych w celu prowadzenia czynności wykrywczych lub identyfikacyjnych.

2. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. a–f oraz i, są przechowywane w zbiorach danych daktyloskopijnych i wykorzystywane w celu prowadzenia czynności wykrywczych.

3. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. j, są przetwarzane w zbiorach danych daktyloskopijnych w celu wyeliminowania, spośród wszystkich zebranych w toku prowadzonego postępowania, śladów pozostawionych przez osoby, o których mowa w art. 20 ust. 1l.

Art. 21l. 1. W weryfikacji, o której mowa w art. 16 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, uczestniczą jednostki organizacyjne Policji, służby, instytucje państwowe lub organy władzy publicznej, które przekazały informacje, w tym dane osobowe, do zbiorów danych daktyloskopijnych.

2. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. a–c, e i f, usuwa się ze zbiorów danych daktyloskopijnych, w przypadku gdy:

1) zostało umorzone postępowanie z uwagi na to, że:
   a) czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia,
   b) zdarzenie lub okoliczność, w związku z którymi wprowadzono dane osobowe do zbioru danych, nie ma znamion czynu zabronionego;
2) osoba, której dane dotyczą:
   a) została uniewinniona prawomocnym wyrokiem sądu,
   b) ukończyła 100. rok życia,
   c) zmarła;
3) utracą swoją przydatność eliminacyjną, jednakże nie dłużej niż po upływie 5 lat od dnia ustania stosunku służbowego lub pracy – w przypadku osób, o których mowa w art. 20 ust. 1o.

3. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. g, usuwa się ze zbiorów danych daktyloskopijnych, jeżeli osoba, której dane dotyczą:

1) uzyskała obywatelstwo polskie;
2) ukończyła 100. rok życia;
3) zmarła.

4. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1, usuwa się ze zbiorów danych daktyloskopijnych po uzyskaniu wiarygodnej informacji.

Art. 21m. 1. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. i, usuwa się ze zbiorów danych daktyloskopijnych po upływie okresu przedawnienia karalności przestępstwa, na wniosek organu prowadzącego postępowanie karne.

2. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. h, usuwa się ze zbiorów danych daktyloskopijnych, w przypadku odnalezienia lub ustalenia miejsca pobytu osoby zaginionej lub po upływie 55 lat od dnia rozpoczęcia ich przetwarzania w zbiorach danych daktyloskopijnych. Informacje te, w tym dane osobowe, usuwa się na wniosek jednostki organizacyjnej, służby, instytucji państwowej lub organu władzy publicznej prowadzącej poszukiwanie.

Art. 21n. Usunięcia informacji, w tym danych osobowych, ze zbioru danych daktyloskopijnych, w tym zniszczenia kart daktyloskopijnych i chejroskopijnych, dokonuje komisja powołana przez Komendanta Głównego Policji, sporządzając z tych czynności protokół.”;

15) po art. 21n dodaje się art. 21na i art. 21nb w brzmieniu:

„Art. 21na. Zadania, o których mowa w art. 21a–21e oraz art. 21h–21n, Komendant Główny Policji realizuje przy pomocy Centralnego Laboratorium Kryminalistycznego Policji.

Art. 21nb. 1. Komendant Główny Policji prowadzi Krajowy System Informacyjny Policji, zwany dalej „KSIP”, będący zestawem zbiorów danych, w którym przetwarza się informacje, w tym dane osobowe, w związku z realizacją zadań ustawowych.

2. W odniesieniu do informacji, w tym danych osobowych, przetwarzanych w KSIP Komendant Główny Policji jest administratorem w rozumieniu przepisów o ochronie danych osobowych.

3. Komendant Główny Policji zapewnia utrzymanie, rozbudowę oraz modyfikację KSIP.

4. Utrzymanie, rozbudowa i modyfikacja KSIP są finansowane z budżetu państwa, z części, której dysponentem jest minister właściwy do spraw wewnętrznych.

5. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, parametry funkcjonalne KSIP, sposób jego funkcjonowania, w tym w sytuacjach

awaryjnych, oraz sposób utrzymania, mając na uwadze potrzebę zapewnienia optymalnego poziomu jego funkcjonowania.”;

16) po art. 46a dodaje się art. 46b w brzmieniu:

„Art. 46b. 1. Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w Policji, przenoszenia do służby w Policji oraz w zakresie wynikającym z przebiegu stosunku służbowego policjantów, także po jego ustaniu, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia (UE) 2016/679, z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 tego rozporządzenia, w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności.

3. Administratorem danych osobowych, o których mowa w ust. 1, w zakresie, w jakim przetwarza te dane, jest Komendant Główny Policji, Komendant CBŚP, Komendant BSWP, dyrektor Centralnego Laboratorium Kryminalistycznego Policji, komendanci wojewódzcy (Stołeczny) Policji, Komendant-Rektor Wyższej Szkoły Policji w Szczytnie oraz komendanci szkół policyjnych.”;

17) w art. 145j:

a) w ust. 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:

„7) krajowego punktu dostępu do systemu Eurodac, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi

Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniającym rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona) (Dz. Urz. UE L 180 z 29.06.2013, str. 1), zwanym dalej „rozporządzeniem (UE) 603/2013”.”,

b) po ust. 5a dodaje się ust. 5b w brzmieniu:

„5b. Do zadań krajowego punktu dostępu do systemu Eurodac, o którym mowa w ust. 1 pkt 7, należy:

1) przesyłanie do systemu Eurodac danych daktyloskopijnych wraz z właściwymi numerami referencyjnymi zgodnie z art. 24 ust. 1 rozporządzenia (UE) 603/2013;

2) weryfikowanie wyników porównania zgodnie z art. 25 ust. 4 rozporządzenia (UE) 603/2013;

3) komunikowanie się z systemem Eurodac zgodnie z art. 26 rozporządzenia (UE) 603/2013;

4) przekazywanie wyników porównania danych daktyloskopijnych z danymi Eurodac właściwym organom.”,

c) ust. 6 otrzymuje brzmienie:

„6. Zadania, o których mowa w ust. 2, 3 i 5b, Komendant Główny Policji wykonuje przy pomocy Centralnego Laboratorium Kryminalistycznego Policji.”.

Art. 59. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2017 r. poz. 2365, z późn. zm.[9)]) wprowadza się następujące zmiany:

1) w art. 1:

a) w ust. 2 pkt 9 otrzymuje brzmienie:

„9) przetwarzanie informacji, w tym danych osobowych, z zakresu ochrony granicy państwowej, kontroli ruchu granicznego, zapobiegania i przeciwdziałania nielegalnej migracji oraz udostępnianie ich sądom, prokuratorom, organom administracji publicznej i innym organom

---

9) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 650, 730, 894 i 1544.

państwowym, uprawnionym do ich otrzymania na podstawie odrębnych ustaw, w zakresie niezbędnym do realizacji ich zadań;”,

b) ust. 3 otrzymuje brzmienie:

„3. Straż Graniczna w zakresie określonym w ust. 2 i 2a współdziała z właściwymi organami i instytucjami Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi, w tym z Międzynarodową Organizacją Policji Kryminalnej – Interpol.”;

2) w art. 9:

a) ust. 1 otrzymuje brzmienie:

„1. W celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz przestępstw skarbowych, a także wykroczeń oraz wykroczeń skarbowych w zakresie określonym w art. 1 ust. 2 pkt 4 i w art. 1 ust. 2a, funkcjonariusze Straży Granicznej pełnią służbę graniczną, prowadzą działania graniczne, wykonują czynności operacyjno-rozpoznawcze i administracyjno-porządkowe oraz prowadzą postępowania przygotowawcze według przepisów Kodeksu postępowania karnego, a także wykonują czynności na polecenie sądu i prokuratury oraz innych właściwych organów państwowych w zakresie, w jakim obowiązek ten został określony w odrębnych przepisach.”,

b) w ust. 1a wyrazy „ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)” zastępuje się wyrazami „ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. …)”;

3) po art. 9c dodaje się art. 9ca w brzmieniu:

„Art. 9ca. 1. Straż Graniczna w celu ochrony obiektów, o których mowa w art. 9c ust. 1, może wprowadzić nadzór nad terenem użytkowanych obiektów lub terenem przyległym do obiektów w postaci środków technicznych oraz urządzeń elektronicznego systemu monitorującego stan bezpieczeństwa obiektu umożliwiających rejestrację obrazu, a także środków organizacyjnych i technicznych zapewniających identyfikację i kontrolę osób przebywających w użytkowanych obiektach, w tym przepustek zawierających wizerunek twarzy, oraz systemów teleinformatycznych przetwarzających informacje o przepustkach, w tym dane osób, którym je wydano.

2. System monitorujący, o którym mowa w ust. 1, stosuje się jedynie w miejscach i pomieszczeniach, w których zapewnia on realizację celu określonego w ust. 1, z wyłączeniem miejsc przeznaczonych do celów sanitarno-higienicznych.

3. Zarejestrowany obraz przetwarza się wyłącznie do celów, dla których został zebrany, i przechowuje się przez okres nieprzekraczający 1 roku. Dane osób, w tym wizerunek twarzy, wykorzystywane do identyfikacji i kontroli osób przebywających w użytkowanych obiektach, przechowuje się nie dłużej niż jest to konieczne do realizacji tego celu.

4. W przypadku gdy zarejestrowany obraz stanowi dowód w postępowaniu lub powzięto informacje, że może on stanowić dowód w postępowaniu, termin określony w ust. 3 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.”;

4) art. 10a otrzymuje brzmienie:

„Art. 10a. 1. Straż Graniczna w celu realizacji ustawowych zadań jest uprawniona do przetwarzania informacji, w tym danych osobowych, oraz ich wymiany z właściwymi organami i instytucjami Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi, w tym z Międzynarodową Organizacją Policji Kryminalnej – Interpol.

2. Straż Graniczna przetwarza dane osobowe w zakresie niezbędnym do realizacji ustawowych zadań lub wykonywania uprawnień związanych z zapobieganiem i zwalczaniem przestępstw oraz przestępstw skarbowych, a także wykroczeń oraz wykroczeń skarbowych, w tym dane osobowe, o których mowa w art. 14 ust. 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przy czym dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA.

3. Danych osobowych, o których mowa w art. 14 ust. 1 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej.

4. Straż Graniczna przetwarza dane osobowe w zakresie niezbędnym do realizacji ustawowych zadań lub wykonywania uprawnień związanych z prowadzeniem postępowań administracyjnych, dokonywaniem kontroli granicznej, realizacją czynności administracyjno-porządkowych oraz innych kontroli albo czynności, do prowadzenia których funkcjonariusze Straży Granicznej są uprawnieni na podstawie ustaw, w tym

mają prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 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 z późn. zm.[10)]), zwanego dalej „rozporządzeniem (UE) nr 2016/679", z wyłączaniem danych dotyczących kodu genetycznego.

5. W przypadku podejrzanych Straż Graniczna w celach, o których mowa w art. 11 ust. 1 pkt 5c lit. b, pobiera:

1) wymazy ze śluzówki policzków oraz imiona, nazwiska lub pseudonimy, imiona i nazwiska rodowe rodziców tych osób, datę i miejsce urodzenia, adres zamieszkania, numer PESEL, obywatelstwo i płeć;
2) odciski linii papilarnych palców i dłoni oraz imiona, nazwiska lub pseudonimy, imiona i nazwiska rodowe rodziców tych osób, datę i miejsce urodzenia, oznaczenie i cechy identyfikacyjne dokumentu tożsamości, adres zamieszkania, numer PESEL, obywatelstwo i płeć, oznaczenie i numer sprawy, miejsce i powód daktyloskopowania, obrazy odcisków linii papilarnych, rodzaj rejestracji, datę rejestracji.

6. Przetwarzanie danych osobowych przez Straż Graniczną w celach, o których mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na podstawie ustawy, prawa Unii Europejskiej oraz postanowień umów międzynarodowych.

7. Straż Graniczna, podejmując działania na podstawie informacji, w tym danych osobowych, przetwarzanych przez Międzynarodową Organizację Policji Kryminalnej – Interpol może wystąpić o przekazanie informacji uzupełniających, w zakresie umożliwiającym wykonanie tych działań. Wymiana informacji uzupełniających odbywa się za pośrednictwem komórki organizacyjnej Komendy Głównej Policji wyznaczonej do wykonywania zadań Krajowego Biura Interpolu.

8. Straż Graniczna, w zakresie swojej właściwości, przetwarza informacje, w tym dane osobowe, uzyskane ze zbiorów danych prowadzonych przez inne służby, instytucje państwowe oraz organy władzy publicznej. Służby, instytucje państwowe oraz organy

---

[10)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

władzy publicznej są obowiązane do nieodpłatnego udostępnienia Straży Granicznej informacji, w tym danych osobowych. W szczególności Straż Graniczna jest uprawniona do uzyskiwania informacji, w tym danych osobowych:

1) gromadzonych w administrowanych przez nich zbiorach danych lub rejestrach;
2) uzyskanych przez te służby lub organy w wyniku wykonywania czynności operacyjno-rozpoznawczych, w tym prowadzonej kontroli operacyjnej.

9. Podmioty, o których mowa w ust. 8, mogą wyrazić pisemną zgodę na udostępnianie danych zgromadzonych w zbiorach danych jednostkom organizacyjnym Straży Granicznej, w drodze teletransmisji, bez konieczności składania wniosku pisemnie w postaci papierowej lub elektronicznej, jeżeli jednostki te spełniają łącznie następujące warunki:

1) posiadają urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał;
2) posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania;
3) jest to uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności.

10. Przetwarzanie informacji, w tym danych osobowych, przez Straż Graniczną może mieć charakter niejawny, odbywać się bez zgody i wiedzy osoby, której dotyczą, oraz z wykorzystaniem środków technicznych.

11. Komendant Główny Straży Granicznej jest administratorem danych osobowych przetwarzanych przez Straż Graniczną w celu realizacji ustawowych zadań.

12. Komendant Główny Straży Granicznej może upoważnić do przetwarzania danych osobowych, o których mowa w ust. 11, komendantów oddziałów Straży Granicznej, Komendanta BSWSG, komendantów ośrodków szkolenia Straży Granicznej, komendantów ośrodków Straży Granicznej oraz kierowników komórek organizacyjnych Komendy Głównej Straży Granicznej.

13. Komendant Główny Straży Granicznej może upoważnić osoby, o których mowa w ust. 12, do udzielania i cofania, w jego imieniu, upoważnień do przetwarzania danych osobowych, o których mowa w ust. 11, podległym im pracownikom i funkcjonariuszom Straży Granicznej.

14. Wyłączenia wynikające z przepisów o ochronie danych osobowych nie naruszają prawa osoby do ubiegania się o informacje jej dotyczące, w formie podania

o zaświadczenie, jeżeli osoba wykaże interes prawny w urzędowym potwierdzeniu określonych faktów lub stanu prawnego.

15. Straż Graniczna udostępnia właściwym podmiotom informacje, o których mowa w art. 1 ust. 2 pkt 9, w tym dane osobowe, na wniosek przekazany pisemnie w postaci papierowej lub elektronicznej, który powinien zawierać podstawę prawną, przeznaczenie oraz wskazanie, w zależności od rodzaju informacji, jakie mają zostać udostępnione, przedziału czasowego podlegającego sprawdzeniu, danych osoby, pojazdu, dokumentu podlegających sprawdzeniu, a także podpis upoważnionej osoby.

16. Przepisu ust. 15 nie stosuje się do udostępniania informacji, w tym danych osobowych, podmiotom występującym o ich przekazanie w związku z wykonywaniem przez te podmioty czynności operacyjno-rozpoznawczych lub prowadzeniem postępowań przygotowawczych.

17. Udostępnianie informacji, o których mowa w art. 1 ust. 2 pkt 9, w tym danych osobowych, może nastąpić w drodze teletransmisji, bez konieczności składania pisemnego wniosku, jeżeli odrębne przepisy dotyczące zadań i uprawnień podmiotów, o których mowa w art. 1 ust. 2 pkt 9, przewidują taką możliwość, podmioty spełniają określone w tych przepisach warunki, a Komendant Główny Straży Granicznej wyrazi pisemną zgodę w postaci papierowej lub elektronicznej na taki sposób udostępnienia informacji, w tym danych osobowych.

18. Minister właściwy do spraw wewnętrznych w porozumieniu z Ministrem Sprawiedliwości określi, w drodze rozporządzenia, sposób pobierania wymazów ze śluzówki policzków, gromadzenia odcisków linii papilarnych oraz zdjęć sygnalitycznych osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, osób o nieustalonej tożsamości lub osób usiłujących ukryć swoją tożsamość, warunki przechowywania, wykorzystania i sposób ich przekazywania innym organom uprawnionym na podstawie przepisów odrębnych, a także wzory wykorzystywanych dokumentów, uwzględniając przypadki i sposoby pobierania odcisków linii papilarnych, przeprowadzania wywiadu daktyloskopijnego oraz wykonywania zdjęć sygnalitycznych, a także kierując się potrzebą ochrony tych danych przed nieuprawnionym dostępem.”;

5) w art. 10b:

a) w ust. 1 po wyrazie „przestępstw” dodaje się wyrazy „oraz przestępstw skarbowych”,

b) dodaje się ust. 8 w brzmieniu:

„8. Dane, o których mowa w ust. 1, pobiera się i udostępnia się także organom ścigania państw członkowskich Unii Europejskiej i innych państw, agencjom Unii Europejskiej zajmującym się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol na ich wniosek, jeżeli następuje to w celu ścigania karnego albo w celu ratowania życia i zdrowia ludzkiego.”;

6) w art. 10bb:

a) w ust. 1 po wyrazie „przestępstw” dodaje się wyrazy „oraz przestępstw skarbowych”,

b) ust. 2 otrzymuje brzmienie:

„2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, przepisy art. 10b ust. 2–8 stosuje się.”;

7) w art. 11:

a) w ust. 1:

– po pkt 5b dodaje się pkt 5c–5e w brzmieniu:

„5c) pobierania od osób odcisków linii papilarnych lub wymazu ze śluzówki policzków:

a) w trybie i przypadkach określonych w przepisach Kodeksu postępowania karnego,

b) w celu identyfikacji osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość, jeżeli ustalenie tożsamości w inny sposób nie jest możliwe;

5d) pobierania od cudzoziemców odcisków linii papilarnych w trybie i przypadkach określonych w przepisach odrębnych;

5e) utrwalania wizerunku osób w celu weryfikacji ich tożsamości, identyfikacji osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość;”,

– po pkt 7a dodaje się pkt 7b w brzmieniu:

„7b) obserwowania i rejestrowania przy użyciu środków technicznych obrazu lub dźwięku w miejscach innych niż publiczne w trakcie interwencji;”,

b) ust. 2 otrzymuje brzmienie:

„2. Rada Ministrów określi, w drodze rozporządzenia, sposób i tryb postępowania przy wykonywaniu uprawnień, o których mowa w ust. 1 pkt 4–5c i 5e, oraz wzory dokumentów stosowanych w tych sprawach, a także podmioty uprawnione do zarządzania doprowadzenia i szczegółowe warunki dokonywania doprowadzeń przy użyciu środków transportu, uwzględniając niezbędne środki ostrożności przy wykonywaniu uprawnień, a także skuteczność działań podejmowanych przez Straż Graniczną oraz poszanowanie praw osób, wobec których działania te są podejmowane.”,

c) w ust. 2a w lit. b wyrazy „pkt 7” zastępuje się wyrazami „pkt 7 i 7b”,

d) w ust. 2b wyrazy „o których mowa w ust. 1 pkt 7” zastępuje się wyrazami „o których mowa w ust. 1 pkt 7 i 7b”,

e) po ust. 2d dodaje się ust. 2e i 2f w brzmieniu:

„2e. Użyte w ust. 1 pkt 7b określenie interwencja oznacza włączenie się funkcjonariusza lub funkcjonariuszy Straży Granicznej w tok zdarzenia mogącego naruszać normy prawne i podjęcie działań zmierzających do ustalenia charakteru, rodzaju i okoliczności powstałego zdarzenia oraz przedsięwzięć ukierunkowanych na przywrócenie naruszonego porządku prawnego.

2f. W przypadkach, o których mowa w ust. 1 pkt 7b, funkcjonariusz Straży Granicznej w miarę możliwości uprzedza osobę, wobec której podejmuje czynności, o rejestrowaniu obrazu lub dźwięku.”,

f) w ust. 5a wyrazy „czynności, o których mowa w ust. 1 pkt 7” zastępuje się wyrazami „czynności, o których mowa w ust. 1 pkt 7 i 7b”;

8) po art. 50a dodaje się art. 50b w brzmieniu:

„Art. 50b. 1. Straż Graniczna przetwarza dane osobowe w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w Straży Granicznej, przenoszenia do służby w Straży Granicznej oraz w zakresie wynikającym z przebiegu stosunku służbowego funkcjonariuszy Straży Granicznej, także po jego ustaniu, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia (UE) 2016/679, z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 tego rozporządzenia w zakresie, w jakim przepisy

szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności.

3. Administratorem danych osobowych, o których mowa w ust. 1, w zakresie, w jakim przetwarza te dane, jest Komendant Główny Straży Granicznej, Komendant BSWSG, komendant oddziału Straży Granicznej, komendant ośrodka szkolenia Straży Granicznej lub komendant ośrodka Straży Granicznej.”.

Art. 60. W ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2017 r. poz. 2205 oraz z 2018 r. poz. 317, 1338 i 1563) po art. 43a dodaje się art. 43b w brzmieniu:

„Art. 43b. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest dyrektor urzędu morskiego.”.

Art. 61. W ustawie z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska (Dz. U. z 2018 r. poz. 1471 i 1479) w art. 10b dodaje się ust. 5 w brzmieniu:

„5. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest minister właściwy do spraw środowiska, Główny Inspektor Ochrony Środowiska lub wojewódzki inspektor ochrony środowiska.”.

Art. 62. W ustawie z dnia 28 września 1991 r. o lasach (Dz. U. z 2017 r. poz. 788 oraz z 2018 r. poz. 650, 651, 1479, 1507 i 1669) w art. 47 po ust. 2b dodaje się ust. 2c w brzmieniu:

„2c. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest minister właściwy do spraw środowiska lub Główny Inspektor Straży Leśnej.”.

Art. 63. W ustawie z dnia 13 października 1995 r. – Prawo łowieckie (Dz. U. z 2017 r. poz. 1295 oraz z 2018 r. poz. 50, 650, 651 i 1507) w art. 39 w ust. 2 dodaje się pkt 2a w brzmieniu:

„2a) Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest minister właściwy do spraw środowiska lub komendant wojewódzki Państwowej Straży Łowieckiej.”.

Art. 64. W ustawie z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (Dz. U. poz. 491, z późn. zm.[11)]) w art. 11t uchyla się ust. 9.

Art. 65. W ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2018 r. poz. 755, z późn. zm.[12)]) w art. 28b pkt 8 otrzymuje brzmienie:

„8) Policji – jeżeli jest to konieczne do skutecznego zapobieżenia popełnieniu przestępstwa, jego wykrycia albo ustalenia sprawców i uzyskania dowodów, na zasadach i w trybie określonych w art. 20 ust. 1e i 1f ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.[13)]);”.

Art. 66. W ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652, 1010 i 1387) wprowadza się następujące zmiany:

1) w art. 11 § 1a otrzymuje brzmienie:

„§ 1a. Jeżeli pokrzywdzony złożył wniosek, o którym mowa w art. 168a § 1, sąd, o którym mowa w § 1, przesyła dyrektorowi zakładu karnego lub aresztu śledczego ten wniosek oraz dane zawierające imię, nazwisko i adres pokrzywdzonego. W wypadku, o którym mowa w art. 168a § 6, sąd przesyła również dane zawierające imię, nazwisko i adres świadka.”;

---

11) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. poz. 443 i 943, z 1998 r. poz. 860, z 2006 r. poz. 1592, z 2007 r. poz. 162, z 2010 r. poz. 1228, z 2012 r. poz. 908 oraz z 2018 r. poz. 106, 138, 650 i 1544.

12) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 685, 771, 1000, 1356, 1629 i 1637).

13) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544 i 1669.

2) w art. 116 w § 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:

„7) informowania o zmianie danych podanych przy przyjęciu, o których mowa w art. 79a § 1 zdanie pierwsze.”;

3) w art. 167a § 1 otrzymuje brzmienie:

„§ 1. Przy zwolnieniu z zakładu karnego skazany:

1) informuje o miejscu stałego pobytu lub innym miejscu przebywania po zwolnieniu;

2) otrzymuje, za pokwitowaniem, znajdujące się w depozycie dokumenty, pieniądze, przedmioty wartościowe i inne przedmioty, jeżeli nie zostały zatrzymane albo zajęte w drodze zabezpieczenia lub egzekucji.”.

Art. 67. W ustawie z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych (Dz. U. z 2017 r. poz. 2243 i 2265 oraz z 2018 r. poz. 3, 5 i 1443) po art. 6a dodaje się art. 6b i art. 6c w brzmieniu:

„Art. 6b. § 1. Sądy wojskowe są administratorami danych osobowych przetwarzanych w postępowaniach sądowych.

§ 2. Do przetwarzania danych osobowych w postępowaniach sądowych przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 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, z późn. zm.[14)]), zwanego dalej „rozporządzeniem 2016/679”, nie stosuje się.

§ 3. W związku z przetwarzaniem danych osobowych w postępowaniach sądowych wykonanie obowiązków, o których mowa w art. 13 rozporządzenia 2016/679, następuje przez umieszczenie informacji określonych w art. 13 rozporządzenia 2016/679 na stronie podmiotowej Biuletynu Informacji Publicznej oraz w widocznym miejscu w budynku sądu.

Art. 6c. § 1. Nadzór nad przetwarzaniem danych osobowych w postępowaniach sądowych wykonują:

1) w zakresie działalności wojskowego sądu garnizonowego – prezes wojskowego sądu okręgowego;

---

14) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

2) w zakresie działalności wojskowego sądu okręgowego – Krajowa Rada Sądownictwa.

§ 2. Do nadzoru, o którym mowa w § 1, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych stosuje się odpowiednio.”.

Art. 68. W ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z 2018 r. poz. 928) dotychczasową treść art. 10a oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), przez straż jest komendant straży.”.

Art. 69. W ustawie z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2017 r. poz. 2128, 1137 i 1694) w art. 10 po ust. 5 dodaje się ust. 5a w brzmieniu:

„5a. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest dyrektor urzędu żeglugi śródlądowej.”.

Art. 70. W ustawie z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (Dz. U. z 2018 r. poz. 424 i 730) wprowadza się następujące zmiany:

1) tytuł ustawy otrzymuje brzmienie:

„o przetwarzaniu informacji kryminalnych”;

2) art. 1 i art. 2 otrzymują brzmienie:

„Art. 1. Ustawa określa zasady postępowania przy przetwarzaniu informacji kryminalnych w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania i zwalczania przestępczości, a także podmioty właściwe w tych sprawach.

Art. 2. 1. Na zasadach określonych w niniejszej ustawie informacje kryminalne przetwarza się w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania i zwalczania przestępczości.

2. Informacje kryminalne przetwarza się bez wiedzy i zgody osoby, której dane dotyczą, oraz z zachowaniem zasad ich ochrony określonych w przepisach o ochronie informacji niejawnych.

3. Informacje kryminalne przekazuje się podmiotom uprawnionym, o których mowa w art. 19, w innych celach niż określone w ust. 1, w zakresie niezbędnym dla realizacji ich zadań ustawowych, w szczególności w celu ochrony bezpieczeństwa i porządku publicznego, zapobiegania i zwalczania zdarzeń oraz zagrożeń o charakterze terrorystycznym lub prowadzenia działań kontrterrorystycznych, jeżeli podmioty te są uprawnione na podstawie ustawy do przetwarzania informacji, w tym danych osobowych, wchodzących w zakres informacji kryminalnych w celu realizacji określonego zadania.”;

3) w art. 4 pkt 4 otrzymuje brzmienie:

„4) przetwarzanie informacji kryminalnych – oznacza przetwarzanie w rozumieniu art. 4 pkt 15 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …);”;

4) w art. 5:

a) ust. 1 otrzymuje brzmienie:

„1. Organem administracji rządowej właściwym w sprawach przetwarzania i przekazywania informacji kryminalnych jest Komendant Główny Policji.”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Komendant Główny Policji jest administratorem danych osobowych, przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.”;

5) w art. 6:

a) pkt 1 otrzymuje brzmienie:

„1) przetwarzanie i przekazywanie informacji kryminalnych;”,

b) pkt 4 otrzymuje brzmienie:

„4) zapewnienie bezpieczeństwa przetwarzanym w Centrum informacjom kryminalnym, zgodnie z przepisami ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, 650, 1000, 1083 i 1669).”;

6) w art. 13 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Zakres przetwarzanych informacji kryminalnych obejmuje następujące dane:”;

7) w art. 16 ust. 1 otrzymuje brzmienie:

„1. W bazach danych gromadzi się informacje kryminalne otrzymane od podmiotów zobowiązanych, o których mowa w art. 20, przekazane w odpowiedzi na zapytanie lub z własnej inicjatywy.”;

8) w art. 18 wprowadza się następujące zmiany:

a) uchyla się ust. 1,

b) ust. 2 otrzymuje brzmienie:

„2. W zakresie nieuregulowanym w niniejszej ustawie do przetwarzania i przekazywania informacji kryminalnych stosuje się przepisy ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.”;

9) tytuł rozdziału 4 otrzymuje brzmienie:

„Rozdział 4

Przetwarzanie i analiza informacji kryminalnych”;

10) w art. 29 ust. 2 otrzymuje brzmienie:

„2. Na wniosek organu Policji, o którym mowa w art. 5b ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.[15)]), zwanej dalej „ustawą o Policji”, oraz organu Straży Granicznej, o którym mowa w art. 3c ust. 2 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2017 r. poz. 2365, z późn. zm.[16)]), zwanej dalej „ustawą o Straży Granicznej”, w przypadku udostępnienia informacji kryminalnej w zakresie realizacji zadań ustawowych określonych w art. 5b ust. 1 ustawy o Policji i art. 3c ust. 1 ustawy o Straży Granicznej przepisu ust. 1 nie stosuje się.”;

11) w art. 33 w ust. 1 po pkt 2 dodaje się przecinek i pkt 3 w brzmieniu:

„3) realizacja zadań ustawowych w zakresie ochrony bezpieczeństwa i porządku publicznego, zapobieganie i zwalczanie zdarzeń oraz zagrożeń o charakterze terrorystycznym lub prowadzenie działań kontrterrorystycznych”.

---

15) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544 i 1669.

16) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 650, 730, 854 i 1544.

Art. 71. W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2018 r. poz. 23, z późn. zm.[17)]) wprowadza się następujące zmiany:

1) w art. 175a w § 1:
   a) wprowadzenie do wyliczenia otrzymuje brzmienie:
   „Administratorami danych osobowych:”,
   b) pkt 2 otrzymuje brzmienie:
   „2) referendarzy sądowych, asystentów sędziów, dyrektorów sądów oraz ich zastępców, kuratorów sądowych, aplikantów aplikacji sądowej, aplikantów kuratorskich, urzędników oraz innych pracowników sądów,”,
   c) część wspólna wyliczenia otrzymuje brzmienie:
   „są prezesi i dyrektorzy właściwych sądów oraz Minister Sprawiedliwości, w zakresie realizowanych zadań.”;
2) po art. 175d dodaje się art. 175da–175dd w brzmieniu:

„Art. 175da. Administratorami danych osobowych przetwarzanych w systemach teleinformatycznych obsługujących postępowania sądowe, w systemach teleinformatycznych, w których są prowadzone rejestry sądowe, oraz w systemach teleinformatycznych, w których są prowadzone urządzenia ewidencyjne (sądowe systemy teleinformatyczne), są sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej, prezesi właściwych sądów oraz Minister Sprawiedliwości w ramach realizowanych zadań.

Art. 175db. Administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej są sądy.

Art. 175dc. § 1. Do przetwarzania danych osobowych w postępowaniach sądowych, w rejestrach sądowych albo w sądowych systemach teleinformatycznych nie stosuje się przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 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

---

17) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 3, 5, 106, 138, 771, 848, 1000, 1045, 1443, 1544 i 1669.

rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[18)]), zwanego dalej „rozporządzeniem 2016/679”.

§ 2. W związku z przetwarzaniem danych osobowych w postępowaniach sądowych wykonanie obowiązków, o których mowa w art. 13 rozporządzenia 2016/679, następuje przez umieszczenie informacji określonych w art. 13 rozporządzenia 2016/679 na stronie podmiotowej Biuletynu Informacji Publicznej oraz w widocznym miejscu w budynku sądu.

Art. 175dd. § 1. Nadzór nad przetwarzaniem danych osobowych, których administratorami są sądy, zgodnie z art. 175da i art. 175db, wykonują:

1) w zakresie działalności sądu rejonowego – prezes sądu okręgowego;
2) w zakresie działalności sądu okręgowego – prezes sądu apelacyjnego;
3) w zakresie działalności sądu apelacyjnego – Krajowa Rada Sądownictwa.

§ 2. W ramach nadzoru, o którym mowa w § 1, właściwe organy:

1) rozpatrują skargi osób, których dane osobowe są przetwarzane niezgodnie z prawem;
2) podejmują działania mające na celu upowszechnianie wśród nadzorowanych administratorów i podmiotów przetwarzających wiedzy o obowiązkach wynikających z rozporządzenia 2016/679 oraz ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …);
3) współpracują z innymi organami sprawującymi nadzór nad przetwarzaniem danych osobowych w ramach postępowań prowadzonych przez sądy i trybunały oraz z organami nadzorczymi w rozumieniu art. 51 rozporządzenia 2016/679, w tym dzielą się informacjami oraz świadczą wzajemną pomoc, w celu zapewnienia spójnego stosowania rozporządzenia 2016/679 oraz ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

§ 3. Organy, o których mowa w § 1, są uprawnione do:

1) nakazywania administratorowi lub podmiotowi przetwarzającemu albo ich przedstawicielom dostarczenia wszelkich informacji potrzebnych do realizacji zadań tego organu;

[18)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

2) zawiadamiania administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia rozporządzenia 2016/679 lub ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
3) uzyskiwania od administratora i podmiotu przetwarzającego dostępu do danych osobowych i informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;
4) uzyskiwania dostępu do pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych;
5) wydawania ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów rozporządzenia 2016/679 lub ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
6) udzielania upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów rozporządzenia 2016/679 lub ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
7) wzywania administratora lub podmiotu przetwarzającego do dostosowania przetwarzania danych do przepisów rozporządzenia 2016/679 lub ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

§ 4. Do przyjmowania i rozpatrywania skarg związanych z przetwarzaniem danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej stosuje się odpowiednio przepisy działu I rozdziału 5a.”.

Art. 72. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2018 r. poz. 430, 1650 i 1544) wprowadza się następujące zmiany:

1) w art. 4 w ust. 2 w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu:
„19) przetwarzanie informacji, w tym danych osobowych, w zakresie realizacji zadań wynikających z niniejszej ustawy oraz z odrębnych przepisów.”;

2) art. 29 otrzymuje brzmienie:

„Art. 29. 1. Żandarmeria Wojskowa w celu realizacji ustawowych zadań jest uprawniona do przetwarzania informacji, w tym danych osobowych, oraz ich wymiany z właściwymi organami i instytucjami krajowymi Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi.

2. Żandarmeria Wojskowa w celach, o których mowa w art. 1 pkt 1 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. ...), przetwarza dane osobowe w zakresie niezbędnym do realizacji zadań ustawowych związanych z zapobieganiem i zwalczaniem przestępstw oraz przestępstw skarbowych, a także wykroczeń oraz wykroczeń skarbowych, w tym dane osobowe, o których mowa w art. 14 ust. 1 tej ustawy. Dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA.

3. Żandarmeria Wojskowa w celu realizacji zadań, o których mowa w art. 4 ust. 1 pkt 3a i ust. 4, może przetwarzać dane biometryczne i dane genetyczne, o których mowa w art. 4 pkt 2 i pkt 4 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości:

1) w trybie i w przypadkach określonych w przepisach Kodeksu postępowania karnego;
2) w celu identyfikacji osób o nieustalonej tożsamości oraz usiłujących ukryć swoją tożsamość, jeżeli ustalenie tożsamości w inny sposób nie jest możliwe.

4. Żandarmeria Wojskowa, w zakresie swojej właściwości, przetwarza informacje, w tym dane osobowe, uzyskane ze zbiorów danych prowadzonych przez inne służby, instytucje państwowe oraz organy władzy publicznej. Służby, instytucje państwowe oraz organy władzy publicznej są zobowiązane do nieodpłatnego udostępnienia Żandarmerii Wojskowej informacji, w tym danych osobowych, na podstawie pisemnego wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta terenowej jednostki organizacyjnej Żandarmerii Wojskowej.

5. Podmioty, o których mowa w ust. 4, mogą wyrazić pisemną zgodę na udostępnianie danych zgromadzonych w zbiorach danych jednostkom organizacyjnym Żandarmerii Wojskowej, w drodze teletransmisji, bez konieczności składania pisemnego wniosku, jeżeli jednostki te spełniają łącznie następujące warunki:

1) posiadają urządzenia umożliwiające odnotowanie w systemie, kto, kiedy i w jakim celu oraz jakie dane uzyskał;
2) posiadają zabezpieczenie techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania;
3) jest to uzasadnione specyfiką lub zakresem wykonywania zadań albo prowadzonej działalności.

6. Przetwarzanie informacji, w tym danych osobowych, przez Żandarmerię Wojskową może mieć charakter niejawny, odbywać się bez zgody i wiedzy osoby, której dotyczą, oraz z wykorzystaniem środków technicznych.

7. Komendant Główny Żandarmerii Wojskowej, komendanci terenowych jednostek organizacyjnych oraz komendanci specjalistycznych jednostek organizacyjnych Żandarmerii Wojskowej są administratorami danych osobowych w stosunku do zbiorów danych osobowych utworzonych przez nich i w celu realizacji zadań ustawowych.

8. Komendant Główny Żandarmerii Wojskowej może upoważnić do przetwarzania danych osobowych, o których mowa w ust. 7, szefów komórek organizacyjnych Komendy Głównej Żandarmerii Wojskowej.

9. Komendant Główny Żandarmerii Wojskowej może upoważnić osoby, o których mowa w ust. 8, do udzielania i cofania, w jego imieniu, upoważnień do przetwarzania danych osobowych podległym im żołnierzom i pracownikom Żandarmerii Wojskowej.

10. Komendanci i szefowie jednostek i komórek organizacyjnych, o których mowa w ust. 7 i 8, mogą tworzyć lub likwidować zbiory danych, w których przetwarza się informacje, w tym dane osobowe, w celu realizacji zadań ustawowych.

11. W przypadku likwidowania zbiorów danych, dokonuje tego komisja wyznaczona przez osoby, o których mowa w ust. 10.

12. Komendanci i szefowie jednostek i komórek organizacyjnych, o których mowa w ust. 7 i 8, prowadzą rejestr zbiorów danych, w których przetwarza się informacje, w tym dane osobowe.

13. Żandarmeria Wojskowa udostępnia właściwym podmiotom informacje, o których mowa w art. 4 ust. 2 pkt 19, w tym dane osobowe, na pisemny wniosek, który powinien zawierać podstawę prawną, przeznaczenie, wskazanie okresu oraz zakresu danych podlegających sprawdzeniu, a także podpis upoważnionej osoby.

14. Przepisu ust. 13 nie stosuje się do udostępniania informacji, w tym danych osobowych, podmiotom występującym o ich przekazanie w związku z wykonywaniem przez te podmioty czynności operacyjno-rozpoznawczych lub prowadzeniem postępowań przygotowawczych.

15. Udostępnianie informacji, o których mowa w art. 4 ust. 2 pkt 19, w tym danych osobowych, może nastąpić w drodze teletransmisji, bez konieczności składania pisemnego wniosku, jeżeli odrębne przepisy dotyczące zadań i uprawnień podmiotów, o których mowa w ust. 5, przewidują taką możliwość, podmioty spełniają określone w tych przepisach warunki, a Komendant Główny Żandarmerii Wojskowej wyrazi pisemną zgodę na taki sposób udostępnienia informacji, w tym danych osobowych.

16. Żandarmeria Wojskowa może przetwarzać odciski linii papilarnych lub wymazy ze śluzówki policzków żołnierzy i pracowników Żandarmerii Wojskowej wykonujących czynności służbowe związane z ujawnianiem, zabezpieczaniem lub badaniem śladów związanych z podejrzeniem popełnienia czynu zabronionego – w celach wyeliminowania pozostawionych przez nich śladów.

17. Minister Obrony Narodowej określi, w drodze rozporządzenia:

1) zasady przetwarzania danych biometrycznych oraz danych genetycznych, w tym w szczególności wymazów ze śluzówki policzków, odcisków linii papilarnych oraz zdjęć sygnalitycznych osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, osób o nieustalonej tożsamości lub osób usiłujących ukryć swoją tożsamość, i sposób ich przekazywania innym organom uprawnionym na podstawie przepisów odrębnych, a także wzory wykorzystywanych dokumentów, uwzględniając przypadki i sposoby pobierania odcisków linii papilarnych, przeprowadzania wywiadu daktyloskopijnego oraz wykonywania zdjęć sygnalitycznych, kierując się potrzebą ochrony tych danych przed nieuprawnionym dostępem;
2) tryb pobierania odcisków linii papilarnych lub wymazów ze śluzówki policzków od żołnierzy i pracowników Żandarmerii Wojskowej oraz sposób przeprowadzania

i dokumentowania czynności związanych z ich przetwarzaniem, uwzględniając konieczność wyeliminowania pozostawionych przez nich śladów;

3) zbiory danych, w których Żandarmeria Wojskowa przetwarza dane osobowe, uwzględniając ich przeznaczenie i zakres;

4) kryteria oceny danych pod kątem przesłanek dalszego przetwarzania, kierując się ich przydatnością do realizacji zadań związanych z zapobieganiem i zwalczaniem przestępczości.”.

Art. 73. W ustawie z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2017 r. poz. 2200, z późn. zm.[19)]) wprowadza się następujące zmiany:

1) w art. 55a po ust. 1 dodaje się ust. 1a i 1b w brzmieniu:

„1a. Inspekcja w celach, o których mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest uprawniona do przetwarzania informacji, w tym danych osobowych, oraz ich wymiany z właściwymi organami i instytucjami krajowymi, Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi.

1b. Inspekcja może przekazać dane osobowe państwu trzeciemu lub organizacjom międzynarodowym, na ich wniosek, w przypadku gdy są spełnione warunki przekazywania informacji określone w art. 18a–18d ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2018 r. poz. 484 i ...).”;

2) po art. 56 dodaje się art. 56a w brzmieniu:

„Art. 56a. Administratorem danych osobowych przetwarzanych w związku z realizacją czynności określonych w art. 56 ust. 1, w celach, o których mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jest Główny Inspektor Transportu Drogowego lub wojewódzki inspektor transportu drogowego.”.

---

19) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 12, 79, 138, 650, 1039, 1480, 1481, 1544, 1592 i 1625.

Art. 74. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2017 r. poz. 1920, z późn. zm.[20)]) w art. 34 ust. 1 otrzymuje brzmienie:

„1. W zakresie swojej właściwości Agencje mogą zbierać, także niejawnie, wszelkie dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 14 ust. 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), a także korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je bez wiedzy i zgody osoby, której te dane dotyczą.”.

Art. 75. W ustawie z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych (Dz. U. z 2017 r. poz. 2188 oraz z 2018 r. poz. 3 i 1443) po art. 12 dodaje się art. 12a i art. 12b w brzmieniu:

„Art. 12a. § 1. Sądy administracyjne są administratorami danych osobowych przetwarzanych w postępowaniach sądowych.

§ 2. Do przetwarzania danych osobowych w postępowaniach sądowych przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 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, z późn. zm.[21)]), zwanego dalej „rozporządzeniem 2016/679”, nie stosuje się.

§ 3. W związku z przetwarzaniem danych osobowych w postępowaniach sądowych wykonanie obowiązków, o których mowa w art. 13 rozporządzenia 2016/679, następuje przez umieszczenie informacji określonych w art. 13 rozporządzenia 2016/679 na stronie podmiotowej Biuletynu Informacji Publicznej oraz w widocznym miejscu w budynku sądu.

[20)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 138, 650, 723, 730, 1544, 1560 i 1669.

[21)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

Art. 12b. § 1. Nadzór nad przetwarzaniem danych osobowych przez wojewódzkie sądy administracyjne w postępowaniach sądowych sprawuje Prezes Naczelnego Sądu Administracyjnego.

§ 2. Nadzór nad przetwarzaniem danych osobowych przez Naczelny Sąd Administracyjny w postępowaniach sądowych sprawuje Krajowa Rada Sądownictwa.

§ 3. Do nadzoru, o którym mowa w § 1 i 2, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych stosuje się odpowiednio.”.

Art. 76. W ustawie z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2017 r. poz. 2117 i 2361 oraz z 2018 r. poz. 650, 927, 1338 i 1629) po art. 60 dodaje się art. 60a w brzmieniu:

„Art. 60a. 1. Straż Ochrony Kolei w celu realizacji ustawowych zadań może przetwarzać dane osobowe także bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane:

1) w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia;
2) z rejestrów, ewidencji i zbiorów, do których Straż Ochrony Kolei posiada dostęp na podstawie odrębnych przepisów.

2. Administratorem danych osobowych przetwarzanych przez Straż Ochrony Kolei jest Komendant Straży Ochrony Kolei.”.

Art. 77. W ustawie z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz. U. z 2018 r. poz. 473) w art. 104 w ust. 1 pkt 10 otrzymuje brzmienie:

„10) Policji, o ile są niezbędne w toczącym się postępowaniu lub na potrzeby wykonywania czynności operacyjno-rozpoznawczych na zasadach i w trybie określonym w art. 20 ust. 1d i 1e ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.[22)]);”.

[22)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544 i 1665.

Art. 78. W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2017 r. poz. 1993, z późn. zm.[23)]) w art. 22a ust. 1 otrzymuje brzmienie:

„1. W granicach zadań, o których mowa w art. 2 ust. 1, CBA może przetwarzać dane osobowe, w tym dane wskazane w art. 14 ust. 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), bez wiedzy i zgody osoby, której te dane dotyczą.”.

Art. 79. W ustawie z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2017 r. poz. 1978 i 2405 oraz z 2018 r. poz. 650, 1544 i 1669) w art. 38 ust. 1 otrzymuje brzmienie:

„1. W zakresie swojej właściwości SKW i SWW mogą zbierać, także niejawnie, wszelkie dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 14 ust. 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), a także korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je bez wiedzy i zgody osoby, której te dane dotyczą.”.

Art. 80. W ustawie z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. z 2018 r. poz. 134 i 138) wprowadza się następujące zmiany:

1) w art. 2:
   a) pkt 1 otrzymuje brzmienie:
      „1) bezpośrednim dostępie – rozumie się przez to dokonywanie wpisów oraz wgląd do danych przetwarzanych poprzez Krajowy System Informatyczny (KSI), realizowany w sposób bezpośredni przez organ wskazany w ustawie;”,
   b) pkt 7 otrzymuje brzmienie:
      „7) informacjach uzupełniających – rozumie się przez to wszelkie informacje, wymieniane za pośrednictwem biur SIRENE między krajowymi a zagranicznymi organami uprawnionymi do przetwarzania danych SIS, niezbędne przy dokonywaniu wpisów do Systemu Informacyjnego Schengen

---

[23)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 138, 650, 730, 1544, 1669 i 1693.

lub w celu umożliwienia podjęcia odpowiednich działań, w przypadkach gdy w wyniku przeglądania danych SIS odnaleziono osoby lub przedmioty, których dotyczą wpisy;”,

c) pkt 11 otrzymuje brzmienie:

„11) Krajowym Systemie Informatycznym (KSI) – rozumie się przez to zespół współpracujących ze sobą urządzeń, procedur przetwarzania informacji i narzędzi programowych (oprogramowania) zastosowanych w celu przetwarzania danych oraz infrastrukturę telekomunikacyjną, umożliwiające organom administracji publicznej i organom wymiaru sprawiedliwości przetwarzanie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym;”,

d) pkt 14 otrzymuje brzmienie:

„14) pośrednim dostępie – rozumie się przez to dokonywanie wpisów oraz wgląd do danych przetwarzanych poprzez Krajowy System Informatyczny (KSI), realizowany w sytuacjach wskazanych w ustawie za pośrednictwem centralnego organu technicznego KSI albo organu wskazanego w art. 7 ust. 2;”,

e) pkt 18 otrzymuje brzmienie:

„18) przetwarzaniu danych – rozumie się przez to przetwarzanie danych będących danymi osobowymi, jak również jakiekolwiek operacje wykonywane na danych niebędących danymi osobowymi, takie jak: zbieranie, wpisywanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. W odniesieniu do danych osobowych przetwarzanych w celach, o których mowa w art. 1 pkt 1 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), stosuje się przepisy tej ustawy, a w przypadku danych osobowych przetwarzanych w innych celach przepisy rozporządzenia 2016/679;”,

f) dodaje się pkt 19 w brzmieniu:

„19) rozporządzeniu 2016/679 – rozumie się przez to rozporządzenie 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, z późn. zm.[24)]).”;

2) tytuł rozdziału 2 otrzymuje brzmienie:

„Rozdział 2

Organy i służby uprawnione do przetwarzania danych”;

3) w art. 6 pkt 4 otrzymuje brzmienie:

„4) sprawdzenia na przejściach granicznych tożsamości posiadacza wizy, autentyczności wizy lub spełnienia warunków wjazdu na terytorium Państw Członkowskich zgodnie z art. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz. Urz. UE L 77/1 z 23.03.2016) przysługuje Straży Granicznej i Służbie Celno-Skarbowej;”;

4) art. 8–10 otrzymują brzmienie:

„Art. 8. Prezes Urzędu Ochrony Danych Osobowych jest uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu sprawowania kontroli.

Art. 9. Prezes Urzędu Ochrony Danych Osobowych w przypadku, o którym mowa w art. 34 ust. 4 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz w art. 49 ust. 4 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), jest organem uprawnionym do przekazania sprawy Europejskiemu Inspektorowi Ochrony Danych, w celu podjęcia działań mediacyjnych.

Art. 10. 1. Administratorem danych osobowych przetwarzanych poprzez Krajowy System Informatyczny (KSI) jest Centralny organ techniczny KSI.”;

5) użyty w tytule rozdziału 3, w art. 11 w ust. 1, w art. 22 w ust. 3, w art. 23 w ust. 4, w art. 24, w art. 25 w ust. 1–4, w art. 27 w ust. 1 w pkt 4 i 5, w art. 27 w ust. 2 w pkt 1, 5 i 9 oraz w art. 28 w różnym przypadku wyraz „wykorzystywania” zastępuje się użytym w odpowiednim przypadku wyrazem „przetwarzania”;

[24)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

6) w art. 11 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Decyzje podejmowane przez właściwe organy w celu rozpatrzenia wniosku wizowego, sprawdzenia autentyczności wizy lub spełnienia warunków wjazdu lub pobytu na terytorium Rzeczypospolitej Polskiej lub Państw Członkowskich mogą się opierać wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych.”;

7) w art. 25 w ust. 3 wyrazy „Generalnego Inspektora Ochrony Danych Osobowych” zastępuje się wyrazami „Prezesa Urzędu Ochrony Danych Osobowych”;

8) art. 30–32 otrzymują brzmienie:

„Art. 30. 1. Centralny organ techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego (KSI), jest obowiązany do wystąpienia do Prezesa Urzędu Ochrony Danych Osobowych z wnioskiem o przeprowadzenie kontroli w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w przepisach o ochronie danych osobowych.

2. Wniosek, o którym mowa w ust. 1, powinien zawierać opis środków technicznych i organizacyjnych, w szczególności w zakresie zapobiegania dostępowi osób nieuprawnionych do Krajowego Systemu Informatycznego (KSI).

3. Centralny organ techniczny KSI jest obowiązany współpracować z Prezesem Urzędu Ochrony Danych Osobowych w celu przeprowadzenia kontroli, o której mowa w ust. 1, w szczególności udzielać informacji i wyjaśnień.

4. W celu wykonania zadań, o których mowa w ust. 1, Prezes Urzędu Ochrony Danych Osobowych, zastępca Prezesa Urzędu Ochrony Danych Osobowych lub upoważnieni przez niego pracownicy Urzędu mają prawo:

1) wstępu, w godzinach od 6.00 do 22.00, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym jest zlokalizowany Krajowy System Informatyczny (KSI), i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych;
2) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii;
4) przeprowadzania oględzin poszczególnych elementów Krajowego Systemu Informatycznego (KSI), w tym urządzeń, oprogramowania, procedur przetwarzania informacji;

5) zlecać sporządzanie ekspertyz i opinii.

5. Prezes Urzędu Ochrony Danych Osobowych po przeprowadzeniu kontroli, o której mowa w ust. 1, przedstawia centralnemu organowi technicznemu KSI pisemną opinię w zakresie spełnienia przez Krajowy System Informatyczny (KSI) wymogów określonych w przepisach o ochronie danych osobowych, a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym (KSI) przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej.

Art. 31. 1. W przypadku przedstawienia przez ministra właściwego do spraw wewnętrznych lub Prezesa Urzędu Ochrony Danych Osobowych zaleceń pokontrolnych, centralny organ techniczny KSI ma prawo zgłoszenia na piśmie umotywowanych zastrzeżeń co do przekazanych zaleceń pokontrolnych, w terminie 7 dni od dnia otrzymania zaleceń pokontrolnych.

2. W razie zgłoszenia zastrzeżeń, o których mowa w ust. 1, odpowiednio minister właściwy do spraw wewnętrznych lub Prezes Urzędu Ochrony Danych Osobowych może:

1) uznać zgłoszone zastrzeżenia za niezasadne i podtrzymać zalecenia pokontrolne;
2) uwzględnić zgłoszone zastrzeżenia w części, a w pozostałym zakresie podtrzymać zalecenia pokontrolne;
3) uwzględnić zgłoszone zastrzeżenia w całości i wydać pozytywną opinię.

Art. 32. W przypadku niezgłoszenia przez centralny organ techniczny KSI zastrzeżeń, jak również w przypadku nieuwzględnienia zastrzeżeń przez odpowiednio ministra właściwego do spraw wewnętrznych lub Prezesa Urzędu Ochrony Danych Osobowych, centralny organ techniczny KSI jest obowiązany wykonać zalecenia pokontrolne, a następnie wystąpić z wnioskiem do organu, który przedstawił zalecenia pokontrolne, o przeprowadzenie kontroli, o której mowa w art. 29 ust. 2 lub art. 30 ust. 1.”;

9) w art. 34:

a) ust. 1 otrzymuje brzmienie:

„1. W przypadku dokonywania jakichkolwiek zmian w Krajowym Systemie Informatycznym (KSI) po jego uruchomieniu centralny organ techniczny KSI jest obowiązany przed wdrożeniem tych zmian do uzyskania pisemnej opinii ministra właściwego do spraw wewnętrznych w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 4 i art. 9 rozporządzenia (WE)

nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz w art. 4 i art. 9 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), oraz w opinii Prezesa Urzędu Ochrony Danych Osobowych.”,

b) ust. 5 otrzymuje brzmienie:

„5. Uzyskanie opinii Prezesa Urzędu Ochrony Danych Osobowych, o której mowa w ust. 1, następuje w zakresie i w trybie określonych w art. 30–32.”.

Art. 81. W ustawie z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. z 2017 r. poz. 1160 oraz z 2018 r. poz. 138 i 310) wprowadza się następujące zmiany:

1) w art. 1 pkt 4 otrzymuje brzmienie:

„4) zasady przetwarzania informacji dotyczących bezpieczeństwa imprez masowych, w tym danych osobowych;”;

2) art. 10 otrzymuje brzmienie:

„Art. 10. Organizator masowej imprezy sportowej, innej niż wymieniona w rozdziale 3, może odmówić na nią wstępu i przebywania osobie, której dane znajdują się w zbiorze danych, o którym mowa w art. 37 pkt 2, lub objętej zakazem klubowym lub zakazem zagranicznym.”;

3) w art. 11 w ust. 3 po wyrazach „co najmniej 30 dni,” dodaje się wyrazy „nie dłużej jednak niż 90 dni,”;

4) w art. 13:

a) ust. 2b i 2c otrzymują brzmienie:

„2b. Administratorami danych osobowych przetwarzanych w systemach, o których mowa w ust. 2a, są właściwe podmioty zarządzające tymi rozgrywkami.

2c. Kompatybilność oznacza, iż elektroniczne systemy, o których mowa w ust. 2, muszą być podłączone do systemów, o których mowa w ust. 2a, oraz działać na podstawie numeru PESEL, a w razie gdy nie został on nadany – rodzaju, serii i numeru dokumentu potwierdzającego tożsamość, po przekazaniu danych osobowych, o których mowa w ust. 4.”,

b) w ust. 4 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Zakres przetwarzanych danych osobowych osób uczestniczących w meczu piłki nożnej obejmuje:”,

c) ust. 7–14 otrzymują brzmienie:

„7. Przetwarzanie informacji, w tym danych osobowych, w systemach, o których mowa w ust. 2 i 2a, ma na celu zapewnienie bezpieczeństwa osób uczestniczących w meczu piłki nożnej.

8. Zakres informacji, w tym danych osobowych, przetwarzanych w systemie, o którym mowa w ust. 2a pkt 1, obejmuje:

1) dane osobowe określone w ust. 4,
2) dane osobowe, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c
3) informacje o zastosowanych zakazach, w tym przekazane przez organizatorów imprez masowych

– w zakresie, w jakim te informacje, w tym dane osobowe, dotyczą uczestników meczów piłki nożnej rozgrywanych w ramach najwyższej ligowej klasy rozgrywkowej rywalizacji mężczyzn.

9. Zakres informacji, w tym danych osobowych, przetwarzanych w systemie, o którym mowa w ust. 2a pkt 2, obejmuje:

1) dane osobowe określone w ust. 4,
2) dane osobowe, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c,
3) informacje o zastosowanych zakazach, w tym przekazane przez organizatorów imprez masowych

– w zakresie, w jakim te informacje, w tym dane osobowe, dotyczą uczestników meczów piłki nożnej rozgrywanych w drugiej i trzeciej najwyższej ligowej klasie rozgrywkowej rywalizacji mężczyzn.

10. Informacje, w tym dane osobowe, do systemów, o których mowa w ust. 2 i 2a, przekazują w zakresie swojej właściwości:

1) właściwy polski związek sportowy;
2) właściwy podmiot zarządzający rozgrywkami;
3) organizator meczu piłki nożnej;
4) Komendant Główny Policji;
5) podmiot uprawniony do dystrybucji biletów.

11. Podmioty przekazujące informacje, w tym dane osobowe, do systemów, o których mowa w ust. 2 i 2a, są odpowiedzialne za kompletność, aktualność oraz prawdziwość przekazywanych informacji.

12. Dostęp do informacji, w tym danych osobowych, przetwarzanych w systemach, o których mowa w ust. 2 i 2a, w zakresie swoich kompetencji, posiadają:

1) właściwy polski związek sportowy;
2) właściwy podmiot zarządzający rozgrywkami;
3) organizator meczu piłki nożnej;
4) podmiot uprawniony do dystrybucji biletów;
5) Policja, w zakresie weryfikacji poprawności informacji o osobach, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c, oraz w związku z prowadzonym postępowaniem przygotowawczym lub czynnościami operacyjno-rozpoznawczymi.

13. Informacje, w tym dane osobowe, przetwarzane w systemach, o których mowa w ust. 2 i 2a, są przechowywane nie dłużej niż przez okres 2 lat od dnia ostatniego zakupu biletu wstępu przez uczestnika meczu piłki nożnej lub przekazania mu innego dokumentu uprawniającego do przebywania na meczu piłki nożnej.

13a. Jeżeli informacje, w tym dane osobowe, przetwarzane w systemach, o których mowa w ust. 2 i 2a, dotyczą osoby, wobec której zostało wydane orzeczenie lub zakaz, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c, wówczas okres, o którym mowa w ust. 13, liczy się od dnia upływu okresu obowiązywania zakazu lub okresu, na który orzeczono dany środek.

14. Informacje, w tym dane osobowe, przetwarzane w systemach, o których mowa w ust. 2 i 2a, podlegają usunięciu, jeżeli:

1) zostały zgromadzone z naruszeniem ustawy;
2) okazały się niekompletne, nieaktualne lub nieprawdziwe;
3) upłynął okres, o którym mowa w ust. 13.”;

5) w art. 15:
   a) w ust. 1 po wyrazie „danych” dodaje się wyraz „osobowych”,
   b) w ust. 2 po wyrazie „dane” dodaje się wyraz „osobowe”.

6) tytuł rozdziału 7 otrzymuje brzmienie:

„Rozdział 7

Zasady przetwarzania informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprezy masowej”;

7) art. 35 otrzymuje brzmienie:

„Art. 35. 1. Przetwarzanie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych odbywa się w celu zapobiegania przestępstwom i wykroczeniom związanym z tymi imprezami oraz ich zwalczania.

2. Przetwarzanie danych osobowych może odbywać się bez obowiązku informowania osób, których one dotyczą.”;

8) w art. 36 ust. 1 i 2 otrzymują brzmienie:

„1. Organem administracji rządowej właściwym w sprawach przetwarzania informacji, w tym danych osobowych, dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, jest Komendant Główny Policji, zwany dalej „Komendantem”.

2. Komendant przetwarza informacje, w tym dane osobowe, dotyczące imprez masowych innych niż masowe imprezy sportowe, w tym mecze piłki nożnej, w zakresie obejmującym dane osobowe o osobach, o których mowa w art. 22 ust. 1 pkt 1 lit. a i b, oraz o terminach i miejscach przeprowadzania tych imprez.”;

9) art. 37 otrzymuje brzmienie:

„Art. 37. Do zadań Komendanta należy w szczególności:

1) przetwarzanie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych;
2) prowadzenie zbioru danych dotyczących bezpieczeństwa imprez masowych;
3) opracowywanie analiz informacji dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej;
4) zapewnienie bezpieczeństwa przetwarzanych informacji dotyczących bezpieczeństwa imprez masowych, w tym, zgodnie z przepisami ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), bezpieczeństwa danych osobowych;
5) współpraca z podmiotami zagranicznymi w zakresie, o którym mowa w pkt 1–3.”;

10) w art. 38:

a) w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Podmiotami uprawnionymi w zakresie swoich kompetencji do otrzymywania od Komendanta informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych, zwanymi dalej „podmiotami uprawnionymi", są:",

b) ust. 2 i 3 otrzymują brzmienie:

„2. Organizatorzy imprez masowych innych niż masowe imprezy sportowe, w tym mecze piłki nożnej, są uprawnieni w zakresie swoich zadań ustawowych do otrzymywania od Komendanta informacji, w tym danych osobowych, dotyczących osób, o których mowa w art. 22 ust. 1 pkt 1 lit. a i b.

3. Komendanci wojewódzcy (Komendant Stołeczny) Policji i komendanci powiatowi (rejonowi, miejscy) Policji przekazują podmiotom, o których mowa w ust. 1 pkt 1–15, na wniosek tych podmiotów, informacje, w tym dane osobowe, o których mowa w art. 36 ust. 2 i art. 40, dotyczące imprez masowych organizowanych na obszarze działania tych komendantów. Przepisy art. 42 ust. 1, 4 i 5, art. 43, art. 44 ust. 1, 2 i 4, art. 45, art. 46 oraz art. 47 stosuje się odpowiednio.";

11) art. 39 otrzymuje brzmienie:

„Art. 39. 1. Podmiotami zobowiązanymi do przekazywania Komendantowi informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych, zwanymi dalej „podmiotami zobowiązanymi", są podmioty, o których mowa w art. 38 ust. 1 pkt 1–15, oraz:

1) Biuro Informacyjne Krajowego Rejestru Karnego oraz sądy, w których zapadło prawomocne orzeczenie o ukaraniu za wykroczenie karą inną niż kara aresztu;
2) związki sportowe;
3) organizatorzy;
4) właściciele obiektów, na terenie których organizowane są masowe imprezy sportowe, w tym mecze piłki nożnej;
5) organizatorzy turystyki;
6) krajowi przewoźnicy realizujący publiczny transport zbiorowy.

2. Podmioty zobowiązane przekazują komendantom wojewódzkim (Komendantowi Stołecznemu) Policji i komendantom powiatowym (rejonowym, miejskim) Policji, na wniosek komendantów, informacje, w tym dane osobowe, o których mowa w art. 36 ust. 2 i art. 40, dotyczące imprez masowych organizowanych

na obszarze działania tych komendantów. Przepisy art. 41, art. 42 ust. 1–3 oraz art. 45 stosuje się odpowiednio.”;

12) w art. 40 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Zakres przetwarzanych informacji, w tym danych osobowych, dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, zawiera dane:”;

13) art. 41–43 otrzymują brzmienie:

„Art. 41. 1. Podmioty zobowiązane, z zastrzeżeniem ust. 2, przekazują Komendantowi informacje, w tym dane osobowe, dotyczące bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, niezwłocznie po ich otrzymaniu, nie później jednak niż w ciągu 24 godzin od chwili ich otrzymania.

2. Podmioty zobowiązane, o których mowa w:

1) art. 38 ust. 1 pkt 13 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 3–5 i 9;
2) art. 38 ust. 1 pkt 15 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 3–7 i 9;
3) art. 39 pkt 2 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 3–5 i 9;
4) art. 39 pkt 3 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 3, 6–10;
5) art. 39 pkt 4 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 4 i 7;
6) art. 39 pkt 5 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 8 i 9;
7) art. 39 pkt 6 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 4, 8 i 9.

Art. 42. 1. Informacje, w tym dane osobowe, dotyczące bezpieczeństwa imprezy masowej przekazuje się za pomocą środków komunikacji elektronicznej albo przez bezpośrednie doręczenie do najbliższego komisariatu lub komendy powiatowej (miejskiej, rejonowej) Policji.

2. Podmioty zobowiązane przekazują informacje, w tym dane osobowe, na kartach rejestracyjnych.

3. Podmioty uprawnione w celu uzyskania informacji, w tym danych osobowych, kierują zapytania, wraz z uzasadnieniem, do Komendanta na kartach zapytania.

4. Komendant udziela informacji na kartach odpowiedzi.

5. Komendant może przekazać informacje, w tym dane osobowe, dotyczące bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, podmiotowi zobowiązanemu, niebędącemu podmiotem uprawnionym, na jego pisemne zapytanie, jeżeli dotyczy ono ustawowych obowiązków tego podmiotu.

6. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób przekazywania informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych przez podmioty zobowiązane, wzory kart rejestracyjnych, karty zapytania oraz karty odpowiedzi, biorąc pod uwagę dane, jakie muszą znaleźć się na kartach, oznaczenia podmiotu uprawnionego oraz podmiotu zobowiązanego, treść informacji, o której mowa w ust. 2, oraz zapytania, o którym mowa w ust. 3, jak również uzasadnienia, o którym mowa w art. 43, a także konieczność zapewnienia bezpieczeństwa przekazywanych informacji, w tym dane osobowe, w szczególności przed dostępem osób nieuprawnionych.

Art. 43. 1. Komendant przekazuje informacje, w tym dane osobowe, dotyczące bezpieczeństwa imprez masowych niezwłocznie po otrzymaniu od podmiotu uprawnionego zapytania wraz z uzasadnieniem. Uzasadnienie powinno wskazywać powód wystąpienia z zapytaniem.

2. Jeżeli zapytanie nie zawiera uzasadnienia lub jest ono niewystarczające, Komendant zwraca się do podmiotu uprawnionego, o którym mowa w ust. 1, o sporządzenie uzasadnienia lub jego uzupełnienie o stosowne informacje.

3. W przypadku gdy przetwarzane w zbiorze danych informacje, w tym dane osobowe, dotyczące bezpieczeństwa imprez masowych są niewystarczające do udzielenia odpowiedzi na zapytanie, Komendant występuje z zapytaniem do podmiotów zobowiązanych w zakresie koniecznym do udzielenia odpowiedzi. Podmiot zobowiązany, do którego Komendant wystąpił z zapytaniem, jest obowiązany niezwłocznie udzielić odpowiedzi w zakresie określonym w art. 41.”;

14) art. 45 otrzymuje brzmienie:

„Art. 45. Treść zapytania skierowanego przez Komendanta lub do Komendanta, a także treść odpowiedzi podmiotu zobowiązanego lub Komendanta podlega zarejestrowaniu w zbiorze danych, o którym mowa w art. 37 pkt 2.”;

15) art. 46–49 otrzymują brzmienie:

„Art. 46. Przetwarzanie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych może być dokonywane przy wykorzystaniu urządzeń i systemów teleinformatycznych, kartotek, wykazów i zbiorów ewidencyjnych.

Art. 47. 1. Podmiot zobowiązany, który stwierdził nieprawidłowość przekazywanej przez siebie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych, zawiadamia o tym niezwłocznie Komendanta.

2. W przypadku, o którym mowa w ust. 1, Komendant niezwłocznie zawiadamia o nieprawidłowości informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych podmioty uprawnione, które tę informację od niego otrzymały.

Art. 48. Informacje, w tym dane osobowe, dotyczące bezpieczeństwa imprez masowych Komendant przechowuje przez okres 10 lat.

Art. 49. Informacje, w tym dane osobowe, dotyczące bezpieczeństwa imprez masowych podlegają niezwłocznemu usunięciu ze zbioru danych, jeżeli:

1) przetwarzanie ich jest zabronione;
2) stały się nieaktualne;
3) okazały się nieprawdziwe;
4) upłynął okres, o którym mowa w art. 48.”;

16) w art. 50 ust. 2 i 3 otrzymują brzmienie:

„2. Komendant w celu zapobiegania i zwalczania przejawów przemocy i chuligaństwa w czasie imprez masowych, a w szczególności meczów piłki nożnej, może przekazywać informacje, w tym dane osobowe, dotyczące bezpieczeństwa imprez masowych instytucjom zagranicznym, w tym zwłaszcza informacje niezbędne do zapewnienia porządku i bezpieczeństwa podczas organizowanych imprez masowych o charakterze międzynarodowym.

3. Do przekazywania informacji, w tym danych osobowych, instytucjom zagranicznym stosuje się odpowiednio przepisy niniejszego rozdziału, chyba że przepisy szczególne stanowią inaczej.”.

Art. 82. W ustawie z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. z 2018 r. poz. 1542 i 1669) wprowadza się następujące zmiany:

1) w art. 2 w ust. 2 po pkt 7 dodaje się pkt 7a w brzmieniu:

„7a) prowadzenie Centralnej Bazy Danych Osób Pozbawionych Wolności, zwanej dalej „Centralną Bazą;”;

2) art. 24 otrzymuje brzmienie:

„Art. 24. 1. Służba Więzienna, w celu realizacji zadań, o których mowa w art. 2 ust. 1, 2 i 2b, oraz zadań wynikających z odrębnych ustaw, jest uprawniona do przetwarzania:

1) informacji innych niż dane osobowe,
2) danych osobowych, a w celu realizacji zadań, o których mowa w art. 2 ust. 1 i 2, także danych wrażliwych, w rozumieniu ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …)

– niezbędnych do realizacji tych zadań.

2. Zasady i warunki przetwarzania danych osobowych na podstawie niniejszej ustawy przez Służbę Więzienną w celu wykonywania orzeczeń wydanych w postępowaniu karnym, postępowaniu w sprawach o przestępstwa skarbowe, w sprawach o wykroczenia lub wykroczenia skarbowe oraz wykonywania kar porządkowych i środków przymusu skutkujących pozbawieniem wolności, a także ochrony przed zagrożeniami dla bezpieczeństwa publicznego i porządku publicznego i zapobiegania takim zagrożeniom reguluje ustawa z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z wyjątkami określonymi w niniejszej ustawie.

3. Służba Więzienna może przetwarzać dane osobowe także bez wiedzy i zgody osób, których dane dotyczą.

4. Służba Więzienna może przetwarzać informacje i dane osobowe o następujących osobach:

1) obecnie lub uprzednio pozbawionych wolności w zakładach karnych i aresztach śledczych – w zakresie związanym z pozbawieniem wolności w tych zakładach i aresztach, w tym w zakresie niezbędnym do:
   a) wykonania orzeczenia, zgodnie z zasadami określonymi w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
   b) zapewnienia porządku i bezpieczeństwa w zakładach karnych i aresztach śledczych,
   c) ochrony społeczeństwa przed przestępczością,
   d) wykonania zadań wynikających z odrębnych ustaw;

2) które mają być pozbawione wolności w zakładach karnych i aresztach śledczych, w wykonaniu orzeczenia wydanego przez właściwy organ i przesłanego przez sąd do zakładu karnego lub aresztu śledczego, w celu realizacji czynności, o których mowa w art. 79 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy – w zakresie niezbędnym do wykonania orzeczenia zgodnie z zasadami określonymi w tym kodeksie;
3) wobec których kary, środki karne i środki zabezpieczające są wykonywane w systemie dozoru elektronicznego – w zakresie niezbędnym do wykonania zadania, o którym mowa w art. 2 ust. 2 pkt 9;
4) innych niż wymienione w pkt 1–3, związane z realizacją wobec tych osób czynności przewidzianych w przepisach odrębnych oraz wykonywaniem praw lub obowiązków osób pozbawionych wolności, w tym dane osobowe:
   a) pokrzywdzonych i świadków – w zakresie niezbędnym do realizacji zadań, o których mowa w art. 168a § 1 i 6 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
   b) osób ubiegających się o wstęp oraz opuszczających teren jednostek organizacyjnych – w zakresie niezbędnym do zapewnienia realizacji czynności wykonywanych przez te osoby na terenie jednostek organizacyjnych,
   c) osób zakłócających spokój lub naruszających porządek i bezpieczeństwo jednostek organizacyjnych – w zakresie niezbędnym dla realizacji czynności przewidzianych w przepisach odrębnych,
   d) rodziny oraz innych osób bliskich – w zakresie realizacji praw przewidzianych w przepisach odrębnych;
5) funkcjonariuszach i pracownikach oraz innych osobach pełniących służbę lub zatrudnionych w organach władzy publicznej, dokonujących czynności z udziałem lub wobec osób, o których mowa w pkt 1–3 lub których dane osobowe zawarto w dokumentach przekazanych Służbie Więziennej – w zakresie niezbędnym do wykonania obowiązków i zadań wymienionych w pkt 1–3.

5. Osobie pozbawionej wolności nie udostępnia się:

1) jej akt osobowych, prowadzonych przez administrację zakładu karnego lub aresztu śledczego, z zastrzeżeniem art. 102 pkt 9 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy;

2) informacji przetwarzanych w Centralnej Bazie lub innym zbiorze danych prowadzonym w systemie teleinformatycznym, w zakresie odpowiadającym informacjom zawartym w aktach, o których mowa w pkt 1, uzasadniającym ograniczenie dostępu do tych akt.”;

3) po art. 24 dodaje się art. 24a i art. 24b w brzmieniu:

„Art. 24a. 1. Służba Więzienna udziela informacji i udostępnia dane osobowe o osobach, na pisemny wniosek w postaci papierowej lub elektronicznej, podmiotom ustawowo uprawnionym, w zakresie określonym w ustawach.

2. Służba Więzienna, na pisemny i uzasadniony wniosek osoby najbliższej w postaci papierowej lub elektronicznej, udostępnia dane osobowe osoby obecnie pozbawionej wolności, za pisemną zgodą tej osoby.

3. Służba Więzienna udziela informacji o osobie pozbawionej wolności, która zmarła:

1) podmiotom ustawowo uprawnionym, na zasadach określonych w ust. 1;

2) osobie najbliższej, na pisemny i uzasadniony wniosek tej osoby;

3) osobie innej niż najbliższa, tylko jeżeli zgon nastąpił w zakładzie karnym lub areszcie śledczym, w zakresie informacji o zgonie, jego miejscu i dacie, po wykazaniu w pisemnym wniosku interesu prawnego w potwierdzeniu tych faktów.

4. Przepisy ust. 3 pkt 2 i 3 nie naruszają zasady udostępniania dokumentacji medycznej zmarłego, o której mowa w art. 26 ust. 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318, 1524, 1115 i 1515).

5. Minister Sprawiedliwości określi, w drodze rozporządzenia, tryb i sposób składania oraz wzór wniosku o udzielenie informacji lub udostępnienie danych osobowych o osobie obecnie lub uprzednio pozbawionej wolności w zakładzie karnym lub areszcie śledczym, zawierającego oznaczenie podmiotu ubiegającego się o udzielenie informacji lub udostępnienie danych osobowych, podstawę prawną, zakres udostępnianych danych i udzielanych informacji oraz danych identyfikujących osobę pozbawioną wolności, a w przypadku osoby najbliższej albo osoby innej niż najbliższa – uzasadnienie wniosku, mając na względzie w szczególności zakres uprawnień ustawowych ubiegających się podmiotów.

Art. 24b. 1. Służba Więzienna w związku z realizacją zadań, o których mowa w art. 2 ust. 1, 2 i 2b, oraz zadań wynikających z odrębnych ustaw jest uprawniona do

przetwarzania danych osobowych i informacji o kandydatach do służby w Służbie Więziennej, pracownikach oraz funkcjonariuszach – w zakresie niezbędnym do realizacji postępowania kwalifikacyjnego oraz stosunku pracy i służby w Służbie Więziennej.

2. Przetwarzanie danych osobowych, o których mowa w ust. 1, następuje z wyłączeniem stosowania art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia 2016/79, w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności.

3. Informacji dotyczących danych osobowych funkcjonariuszy oraz pracowników nie udziela się na wniosek osób pozbawionych wolności lub innych podmiotów.

4. Informacje o ograniczeniach w stosowaniu rozporządzenia 2016/679 udostępnia się na stronie podmiotowej Biuletynu Informacji Publicznej Służby Więziennej.”;

4) uchyla się art. 25;

5) po rozdziale 4 dodaje się rozdział 4a w brzmieniu:

„Rozdział 4a

Centralna Baza

Art. 25a. 1. Centralna Baza jest zbiorem informacji i danych osobowych, zwanych w niniejszym rozdziale „informacjami”, użytkowanym przez jednostki organizacyjne i prowadzonym w systemie teleinformatycznym.

2. W Centralnej Bazie przetwarza się informacje niezbędne do realizacji ustawowych zadań wykonywanych przez Służbę Więzienną, dotyczące:

1) osób, o których mowa w art. 24 ust. 4 pkt 1, obejmujące:

   a) dane osobowe, takie jak: imiona, nazwisko, poprzednio używane imiona i nazwiska, pseudonimy, imiona i nazwiska rodziców, nazwisko rodowe matki, datę i miejsce urodzenia, numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), aktualne i poprzednie adresy zameldowania, zamieszkania lub pobytu, także czasowego, obywatelstwo,

   b) informacje pozwalające na identyfikację osoby pozbawionej wolności, w tym dane biometryczne,

c) informacje wynikające z orzeczeń i innych dokumentów przesłanych przez sąd do zakładu karnego lub aresztu śledczego, w tym informacje, o których mowa w art. 11 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,

d) informacje dotyczące stawienia się skazanego lub ukaranego do odbycia kary we właściwym zakładzie karnym lub areszcie śledczym,

e) informacje dotyczące osoby pozbawionej wolności zebrane w trybie art. 14 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,

f) informacje związane z pobytem osoby pozbawionej wolności w zakładzie karnym lub areszcie śledczym, w szczególności:

- informacje o wprowadzonych do wykonania orzeczeniach oraz okresach wykonywania pozbawienia wolności, w tym także poza zakładem karnym lub aresztem śledczym, oraz inne informacje mające wpływ na ustalenie terminu końca kary lub środka przymusu,
- informacje niezbędne do dokonania prawidłowej klasyfikacji, rozmieszczenia wewnątrz zakładu karnego lub aresztu śledczego oraz indywidualnego postępowania zmierzającego do realizacji celów, jakim ma służyć wykonanie kar pozbawienia wolności, środków przymusu skutkujących pozbawieniem wolności oraz tymczasowego aresztowania, w tym w szczególności informacje:
  - o których mowa w art. 82 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
  - wynikające z badań osobopoznawczych, o których mowa w art. 82 § 3 i art. 212c § 1 zdanie pierwsze ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
  - dotyczące diagnoz psychologicznych oraz udzielonej pomocy psychologicznej i terapeutycznej,
- informacje o zakwalifikowaniu osoby pozbawionej wolności jako osoby stwarzającej poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu karnego lub aresztu śledczego,
- informacje o objęciu osoby pozbawionej wolności szczególną ochroną w warunkach zwiększonej izolacji i zabezpieczenia,

- informacje dotyczące zdrowia, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie zdrowia,
- informacje dotyczące wykształcenia, zawodu, innych kwalifikacji zawodowych oraz nauki, w tym miejsca jej pobierania,
- informacje dotyczące wniosków, skarg i próśb złożonych przez osobę pozbawioną wolności,
- oznaczenia i cechy identyfikacyjne dokumentów, w tym dokumentów stwierdzających tożsamość, przekazanych do depozytu zakładu karnego lub aresztu śledczego,
- informacje o rozmieszczeniu wewnątrz zakładu karnego lub aresztu śledczego, przenoszeniu między zakładami karnymi i aresztami śledczymi, o przebywaniu poza terenem tych zakładów lub aresztów pod konwojem, o przepustce lub innym czasowym zezwoleniu na opuszczenie terenu zakładu karnego lub aresztu śledczego, wydaniu poza teren tego zakładu lub aresztu, w tym do udziału w czynnościach procesowych, o ucieczce z zakładu karnego lub aresztu śledczego, a także o tym, że w wyznaczonym terminie osoba pozbawiona wolności nie powróciła z przepustki lub innego czasowego zezwolenia na opuszczenie terenu zakładu karnego lub aresztu śledczego,
- informacje dotyczące zgonu osoby pozbawionej wolności w zakładzie karnym lub areszcie śledczym,
- informacje dotyczące zatrudnienia osoby pozbawionej wolności,
- informacje w zakresie spraw prowadzonych w szczególności w związku z postępowaniem o zezwolenie na odbywanie kary w systemie dozoru elektronicznego, warunkowe przedterminowe zwolnienie oraz przerwę w wykonaniu kary,

g) informacje związane ze zwolnieniem osoby pozbawionej wolności z zakładu karnego lub aresztu śledczego, w tym dotyczące zwolnienia skazanego lub ukaranego na przerwę w wykonaniu kary,

h) inne informacje, jeżeli wynika to z przepisów szczególnych;

2) osób, o których mowa w art. 24 ust. 4 pkt 2, obejmujące informacje, o których mowa w pkt 1 lit. a–d;

3) osób, o których mowa w art. 24 ust. 4 pkt 4, obejmujące:
   a) imię, nazwisko, jeżeli jest to konieczne – adres miejsca zamieszkania,
   b) informacje umożliwiające identyfikację osoby, zawarte w dokumentach stwierdzających tożsamość lub innych dokumentach,
   c) informacje o udzieleniu widzenia lub wykonaniu innych czynności na terenie zakładu karnego lub aresztu śledczego,
   d) inne informacje, jeżeli wynika to z przepisów szczególnych;
4) funkcjonariuszy, pracowników i osób, o których mowa w art. 24 ust. 4 pkt 5, obejmujące tylko informacje konieczne dla prawidłowego przetwarzania informacji w Centralnej Bazie i realizacji, przy wykorzystaniu informacji w tej bazie, ustawowych zadań Służby Więziennej, jeżeli wynika to z przepisów szczególnych.

Art. 25b. 1. Dyrektor Generalny:

1) prowadzi w systemie teleinformatycznym Centralną Bazę;
2) jest administratorem informacji, w tym danych osobowych, przetwarzanych w Centralnej Bazie;
3) dokonuje weryfikacji przydatności informacji w Centralnej Bazie, mając na względzie ich niezbędność do realizacji ustawowych zadań wynikającą z rodzaju informacji oraz upływu czasu;
4) zapewnia:
   a) bezpieczeństwo Centralnej Bazy, w szczególności zabezpiecza przetwarzane w niej informacje przed nieuprawnionym dostępem, zniszczeniem oraz utratą,
   b) utrzymanie i niezbędne modyfikacje Centralnej Bazy.

2. Informacje w Centralnej Bazie:

1) przetwarza się przez okres, w którym są niezbędne do realizacji ustawowych zadań wykonywanych przez Służbę Więzienną. Dyrektor Generalny dokonuje, nie rzadziej niż co 5 lat, weryfikacji potrzeby dalszego przetwarzania tych informacji, ustalając informacje zbędne;
2) uznane za zbędne, mogą być przetwarzane tylko w celu realizacji obowiązku, o którym mowa w pkt 3. Jeżeli przemawia za tym prawidłowość informacji przetwarzanych w Centralnej Bazie, informacje uznane za zbędne mogą być przekształcone w sposób uniemożliwiający przyporządkowanie poszczególnych danych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo

w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań;

3) stanowią materiały archiwalne w rozumieniu art. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r. poz. 217).

3. Utrzymanie i niezbędne modyfikacje Centralnej Bazy są finansowane z budżetu państwa, z części, której dysponentem jest Minister Sprawiedliwości.

4. Dyrektor Generalny powierza, w drodze zarządzenia, o którym mowa w ust. 5, podległym jednostkom organizacyjnym, przetwarzanie danych osobowych w Centralnej Bazie, w zakresie niezbędnym do realizacji ustawowych zadań Służby Więziennej.

5. Dyrektor Generalny określi, w drodze zarządzenia, sposób oraz szczegółowe warunki użytkowania w jednostkach organizacyjnych Centralnej Bazy, w tym warunki powierzenia tym jednostkom danych osobowych przetwarzanych w Centralnej Bazie, mając na względzie prawidłową realizację zadań związanych z przetwarzaniem informacji w Centralnej Bazie oraz jej funkcjonowaniem.

Art. 25c. 1. Jeżeli jest to niezbędne do realizacji zadań ustawowych, o zgodę do Dyrektora Generalnego na wielokrotne, nieograniczone w czasie udostępnianie informacji z Centralnej Bazy, za pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku, mogą wystąpić:

1) sądy powszechne, sądy wojskowe oraz Sąd Najwyższy;
2) organy prokuratury;
3) Komendant Główny Policji;
4) Komendant Główny Straży Granicznej;
5) Komendant Główny Żandarmerii Wojskowej;
6) Komendant Służby Ochrony Państwa;
7) Komendant Straży Marszałkowskiej;
8) Szef Agencji Bezpieczeństwa Wewnętrznego;
9) Szef Agencji Wywiadu;
10) Szef Centralnego Biura Antykorupcyjnego;
11) Szef Krajowej Administracji Skarbowej;
12) Szef Służby Kontrwywiadu Wojskowego;
13) Szef Służby Wywiadu Wojskowego;
14) Minister Obrony Narodowej;
15) Prezes Prokuratorii Generalnej Rzeczypospolitej Polskiej;

16) Rzecznik Praw Obywatelskich.

2. O zgodę, o której mowa w ust. 1, występuje:

1) Minister Sprawiedliwości – w imieniu podmiotów, o których mowa w ust. 1 pkt 1;

2) Prokurator Generalny – w imieniu podmiotów, o których mowa w ust. 1 pkt 2.

Art. 25d. 1. Dyrektor Generalny wyraża zgodę, w drodze decyzji, na wielokrotne, nieograniczone w czasie udostępnianie informacji z Centralnej Bazy, z wyjątkiem informacji dotyczących zdrowia osób obecnie lub uprzednio pozbawionych wolności oraz informacji dotyczących diagnoz psychologicznych oraz udzielonej im pomocy psychologicznej i terapeutycznej, za pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku, podmiotom wymienionym w art. 25c ust. 1, jeżeli podmioty te, z zastrzeżeniem ust. 2, spełniają łącznie następujące warunki:

1) posiadają urządzenia umożliwiające odnotowanie w systemie kto, kiedy, w jakim celu oraz jakie informacje uzyskał;

2) posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie informacji niezgodnie z celem ich uzyskania;

3) jest to uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności;

4) po stronie tych podmiotów oraz Służby Więziennej istnieją warunki techniczne.

2. Warunki udostępniania informacji podmiotowi wymienionemu w art. 25c ust. 1 pkt 15 określa Dyrektor Generalny, w decyzji, o której mowa w ust. 1, mając na względzie:

1) że informacje z Centralnej Bazy udostępniane są Rzecznikowi Praw Obywatelskich lub osobie przez niego upoważnionej na terenie zakładu karnego lub aresztu śledczego;

2) konieczność wprowadzenia zabezpieczeń technicznych i organizacyjnych uniemożliwiających wykorzystanie informacji niezgodnie z celem ich uzyskania;

3) zasady przetwarzania informacji w Centralnej Bazie przez Służbę Więzienną.

3. Informacje z Centralnej Bazy Dyrektor Generalny udostępnia w takim zakresie, określonym w decyzji, o której mowa w ust. 1, w jakim są one niezbędne do realizacji zadań ustawowych.

Art. 25e. Dyrektor Generalny, po wyrażeniu zgody w drodze decyzji, o której mowa w art. 25d ust. 1, umożliwia wielokrotne, nieograniczone w czasie udostępnianie

informacji z Centralnej Bazy, w zakresie określonym w tej decyzji, za pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku.

Art. 25f. 1. Dyrektor Generalny, w drodze decyzji, odmawia wyrażenia zgody na wielokrotne, nieograniczone w czasie, udostępnianie informacji z Centralnej Bazy, za pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku, jeżeli:

1) podmiot występujący z wnioskiem nie jest podmiotem wymienionym w art. 25c ust. 1 pkt 3–15 lub ust. 2;
2) podmiot wymieniony w art. 25c ust. 1 pkt 3–14 lub ust. 2 nie wykazał, że spełnione są warunki określone w art. 25d ust. 1 pkt 1–3;
3) nie istnieją warunki techniczne po stronie podmiotów wymienionych w art. 25c ust. 1 pkt 1–14 lub Służby Więziennej;
4) podmiot wymieniony w art. 25c ust. 1 pkt 15 nie spełnił warunków określonych przez Dyrektora Generalnego, o których mowa w art. 25d ust. 2.

2. Dyrektor Generalny cofa w drodze decyzji zgodę, o której mowa w art. 25d ust. 1, jeżeli zadania podmiotu, który uzyskał zgodę, nie czynią niezbędnym takiego dostępu lub ustalono, że podmiot taki nie spełnia warunków, o których mowa w art. 25d ust. 1–4, albo podmiot wymieniony w art. 25c ust. 1 pkt 15 nie spełnia warunków określonych przez Dyrektora Generalnego, o których mowa w art. 25d ust. 2.

3. Decyzja, o której mowa w ust. 2, podlega natychmiastowemu wykonaniu.

4. Od decyzji, o których mowa w ust. 1 i 2, służy wniosek o ponowne rozpatrzenie sprawy.

Art. 25g. 1. Minister Sprawiedliwości określi, w drodze rozporządzenia:

1) tryb uzyskiwania zgody na udostępnianie informacji z Centralnej Bazy, o której mowa w art. 25c ust. 1;
2) wzór wniosku o udostępnianie informacji z Centralnej Bazy, o którym mowa w art. 25c ust. 1;
3) warunki techniczne i organizacyjne wykonania decyzji, o której mowa w art. 25d ust. 1;
4) sposób i tryb udostępniania informacji z Centralnej Bazy, o którym mowa w art. 25c ust. 1.

2. Wydając rozporządzenie, o którym mowa w ust. 1, Minister Sprawiedliwości uwzględni w szczególności:

1) wymagania, o których mowa w art. 25d ust. 1 pkt 1–4, w tym zwłaszcza konieczność wykazania przez podmioty, o których mowa w art. 25c ust. 1 pkt 3–14 i ust. 2, informacji, których udostępnianie jest niezbędne dla wykonywania zadań określonych w odrębnych ustawach, oraz konieczność wykazania przez te podmioty odpowiedniego poziomu zabezpieczeń technicznych i organizacyjnych;
2) wymagania, o których mowa w art. 25d ust. 2, w przypadku podmiotu wymienionego w art. 25c ust. 1 pkt 15;
3) potrzebę zapewnienia sprawności i bezpieczeństwa udostępniania informacji z Centralnej Bazy, za pośrednictwem systemu teleinformatycznego, oraz ochrony tych informacji przed nieuprawnionym dostępem.

Art. 25h. Minister Sprawiedliwości i minister właściwy do spraw wewnętrznych określą, w drodze rozporządzenia, zakres informacji w Centralnej Bazie, do których bezpośredni dostęp posiada punkt kontaktowy, o którym mowa w art. 4 ust. 1 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2018 r. poz. 484 i ...), w celu ich wymiany z organami ścigania innych państw na zasadach i trybie określonych w przepisach tej ustawy, mając na względzie konieczność zapewnienia dostępu do informacji niezbędnych do wykonywania zadań przez ten punkt kontaktowy oraz potrzebę zapewnienia bezpieczeństwa i ochrony danych osobowych przetwarzanych w Centralnej Bazie.

Art. 25i. Korzystając z informacji z Centralnej Bazy, Dyrektor Generalny:

1) przekazuje, za pośrednictwem systemu teleinformatycznego, informacje o osobach pozbawionych wolności do Krajowego Rejestru Karnego, w zakresie określonym w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2018 r. poz. 1218 i 1544) oraz w przepisach wydanych na podstawie art. 12 ust. 3 tej ustawy;
2) może przekazywać, za pośrednictwem systemu teleinformatycznego, informacje określone w odrębnych przepisach, do uprawnionych podmiotów, realizując ustawowe zadania Służby Więziennej wynikające z tych przepisów.

Art. 25j. Minister Sprawiedliwości w porozumieniu z ministrem właściwym do spraw wewnętrznych oraz Ministrem Obrony Narodowej może określić, w drodze rozporządzenia:

1) sposób oraz warunki przekazywania z Centralnej Bazy informacji, o których mowa w art. 25i pkt 2,

2) zadania Służby Więziennej realizowane w sposób określony w art. 25i pkt 2

– uwzględniając w szczególności potrzebę stworzenia możliwości uproszczenia trybu przekazywania informacji przez organy Służby Więziennej uprawnionym podmiotom, zakres i sposób działania tych podmiotów, potrzebę minimalizowania kosztów realizacji zadań przez organy władzy publicznej oraz konieczność ochrony przekazywanych w tym trybie informacji.”.

Art. 83. W ustawie z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz. U. z 2018 r. poz. 470, z późn. zm.[25)]) w art. 25 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) Komendant Główny Policji – na zasadach i w trybie określonym w art. 20 ust. 1e i 1f ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.[26)]);”.

Art. 84. W ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, 650, 1000, 1083 i 1669) w art. 1 dodaje się ust. 4 i 5 w brzmieniu:

„4. Do danych osobowych stanowiących informacje niejawne nie stosuje się przepisów o ochronie danych osobowych.

5. Do danych osobowych stanowiących informacje niejawne stosuje się przepisy niniejszej ustawy.”.

[25)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 723, 730, 771, 1000 i 1104.

[26)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544 i 1669.

Art. 85. W ustawie z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz. U. z 2018 r. poz. 484) wprowadza się następujące zmiany:

1) tytuł ustawy otrzymuje brzmienie:

„o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi”;

2) w art. 1:

a) ust. 1 otrzymuje brzmienie:

„1. Ustawa określa:

1) zasady i warunki wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej, organami ścigania państw trzecich, agencjami Unii Europejskiej, organizacjami międzynarodowymi w celu rozpoznawania, wykrywania lub zwalczania przestępstw lub przestępstw skarbowych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego oraz zapobiegania takim przestępstwom i zagrożeniom, a także ścigania sprawców przestępstw lub przestępstw skarbowych;

2) podmioty uprawnione w tych sprawach.”,

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Podmiotami uprawnionymi do wymiany informacji z podmiotami, o których mowa w ust. 1 pkt 1, są:”,

c) w ust. 3 uchyla się pkt 1;

3) w art. 3:

a) pkt 1 otrzymuje brzmienie:

„1) pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, aby 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;”,

b) uchyla się pkt 2,

c) pkt 3 otrzymuje brzmienie:

„3) informacji – rozumie się przez to informacje, w tym dane osobowe, do których przetwarzania w celu realizacji swoich zadań ustawowych są uprawnione, na podstawie przepisów odrębnych, podmioty uprawnione;”,

d) uchyla się pkt 7,

e) pkt 8 otrzymuje brzmienie:

„8) wymianie – rozumie się przez to przekazywanie, udostępnianie, uzyskiwanie lub otrzymywanie informacji przez organy ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencje Unii Europejskiej, organizacje międzynarodowe lub podmioty uprawnione;”,

f) dodaje się pkt 9 i 10 w brzmieniu:

„9) organizacji międzynarodowej – rozumie się przez to 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, w szczególności Międzynarodową Organizację Policji Kryminalnej – Interpol;

10) agencji Unii Europejskiej – rozumie się przez to agencję Unii Europejskiej zajmującą się zapobieganiem i zwalczaniem przestępczości.”;

4) art. 4 i art. 5 otrzymują brzmienie:

„Art. 4. 1. W ramach struktury Komendy Głównej Policji wyznacza się komórkę organizacyjną pełniącą funkcję punktu kontaktowego do wymiany informacji między podmiotami uprawnionymi a podmiotami, o których mowa w art. 1 ust. 1 pkt 1, zwaną dalej „punktem kontaktowym”.

2. Dopuszcza się bezpośrednie przekazywanie lub otrzymywanie informacji z pominięciem punktu kontaktowego między przedstawicielami uprawnionych podmiotów a podmiotów, o których mowa w art. 1 ust. 1 pkt 1, podczas prowadzonych wspólnych patroli, spotkań operacyjnych lub innych operacji transgranicznych.

3. Dopuszcza się bezpośrednią wymianę informacji z pominięciem punktu kontaktowego między przedstawicielami uprawnionych podmiotów a podmiotów, o których mowa w art. 1 ust. 1 pkt 1, w ramach:

1) współpracy na terenach przygranicznych, w tym realizowanej przez międzynarodowe centra współpracy;

2) wykonywania zadań oficera łącznikowego podmiotu uprawnionego za granicą lub oficera łącznikowego wchodzącego w skład polskiego biura łącznikowego przy Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol).

4. Nie naruszając przepisów odrębnych, punkt kontaktowy może upoważnić podmioty uprawnione do bezpośredniej wymiany informacji z podmiotami, o których mowa w art. 1 ust. 1 pkt 1. W upoważnieniu punkt kontaktowy określa warunki, zasady i sposób takiej wymiany.

5. Ustawa nie narusza przepisów odrębnych o organizacji i zadaniach innych punktów kontaktowych niż wymieniony w ust. 1.

Art. 5. Do zadań punktu kontaktowego należy:

1) przyjmowanie wniosków o udzielenie informacji składanych przez podmioty, o których mowa w art. 1 ust. 1 pkt 1, oraz udzielanie odpowiedzi na te wnioski;
2) przekazywanie wniosków o udzielenie informacji składanych przez podmioty, o których mowa w art. 1 ust. 1 pkt 1, podmiotom uprawnionym, zgodnie z ich właściwością, w celu udzielenia odpowiedzi na te wnioski;
3) przekazywanie podmiotom, o których mowa w art. 1 ust. 1 pkt 1, wniosków o udzielenie informacji składanych przez podmioty uprawnione;
4) przekazywanie podmiotom, o których mowa w art. 1 ust. 1 pkt 1, informacji w przypadku, o którym mowa w art. 11 ust. 1 pkt 2;
5) koordynowanie wymiany informacji;
6) przetwarzanie, w tym przechowywanie, informacji wymienianych w oparciu o niniejszą ustawę.”;

5) art. 8 otrzymuje brzmienie:

„Art. 8. 1. Punkt kontaktowy wymienia informacje z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, dostępnymi kanałami komunikacji wykorzystywanymi w międzynarodowej współpracy policyjnej, w szczególności udostępnianymi przez:

1) Międzynarodową Organizację Policji Kryminalnej – Interpol;
2) Agencję Unii Europejskiej ds. Współpracy Organów Ścigania (Europol);
3) biura SIRENE.

2. Punkt kontaktowy może przekazywać podmiotom, o których mowa w art. 1 ust. 1 pkt 1, informacje za pośrednictwem oficerów łącznikowych lub innych przedstawicieli podmiotów uprawnionych w podmiotach, o których mowa w art. 1 ust. 1

pkt 1, oraz oficerów łącznikowych lub innych przedstawicieli podmiotów, o których mowa w art. 1 ust. 1 pkt 1, w Rzeczypospolitej Polskiej.”;

6) art. 10 otrzymuje brzmienie:

„Art. 10. Rada Ministrów określi, w drodze rozporządzenia:

1) szczegółowy sposób działania punktu kontaktowego,
2) sposób wyznaczania oraz działania komórek organizacyjnych w podmiocie uprawnionym odpowiedzialnym za wymianę informacji z punktem kontaktowym,
3) sposób rejestrowania wniosków o udzielenie informacji,
4) sposób wymiany informacji między punktem kontaktowym a podmiotami, o których mowa w art. 1 ust. 1 pkt 1, oraz punktem kontaktowym a podmiotami uprawnionymi,
5) wzory formularzy wykorzystywanych do wymiany informacji

– mając na uwadze wymogi zapewnienia efektywnej wymiany informacji przez punkt kontaktowy oraz ciągłości jego funkcjonowania, wdrożenia systemu rejestrowania informacji w punkcie kontaktowym, w tym czasu przekazania lub otrzymania informacji oraz wniosków o przekazanie informacji, a także uwzględniając uregulowania Unii Europejskiej dotyczące ujednoliconych wzorów formularzy wymiany informacji.”;

7) tytuł rozdziału 3 otrzymuje brzmienie:

„Rozdział 3

Warunki i zasady wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej i agencjami Unii Europejskiej”;

8) w art. 11 w ust. 1 pkt 2 otrzymuje brzmienie:

„2) z urzędu przekazują organom ścigania państw członkowskich Unii Europejskiej lub agencjom Unii Europejskiej informacje, jeżeli istnieje uzasadnione przypuszczenie, że informacje te przyczynią się do wykrycia i zatrzymania sprawców przestępstw lub przestępstw skarbowych lub zapobieżenia przestępstwu na terytorium państwa członkowskiego Unii Europejskiej lub państw trzecich, z zastrzeżeniem art. 18d ust. 2.”;

9) w art. 12:

a) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Podmioty uprawnione, przekazując informacje organom ścigania państw członkowskich, zapewniają, aby wymiana danych osobowych nie była ograniczana

ani zakazywana z powodów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.”;

b) uchyla się ust. 2,

c) dodaje się ust. 3 w brzmieniu:

„3. Przekazując informację, podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, wskazują organowi ścigania państwa członkowskiego Unii Europejskiej sposób, w jaki może być ona wykorzystana przez ten organ, w szczególności, czy może być ona wykorzystana w postępowaniu karnym.”;

10) w art. 16:

a) ust. 1 otrzymuje brzmienie:

„1. Podmioty uprawnione przetwarzają informacje uzyskane w wyniku ich wymiany z organami ścigania państw członkowskich Unii Europejskiej w celach wskazanych w art. 1 ust. 1 pkt 1.”,

b) uchyla się ust. 3;

11) w art. 17 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Jeżeli przy przekazywaniu informacji organ ścigania państwa członkowskiego Unii Europejskiej nie zastrzeże inaczej, informacje uzyskane przez podmiot uprawniony w ten sposób mogą zostać wykorzystane w postępowaniu karnym.”;

12) po art. 17 dodaje się art. 17a w brzmieniu:

„Art. 17a. Szczegółowe zasady i warunki wymiany informacji z agencjami Unii Europejskiej przez podmioty uprawnione i punkt kontaktowy określają przepisy Unii Europejskiej.”;

13) uchyla się art. 18;

14) dodaje się rozdział 3a w brzmieniu:

„Rozdział 3a

Warunki i zasady wymiany informacji z organami ścigania państw trzecich i organizacji międzynarodowych

Art. 18a. 1. Dane osobowe mogą zostać przekazane przez podmioty uprawnione lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, do państwa trzeciego lub organizacji międzynarodowej, jeżeli:

1) przekazanie jest niezbędne do celów, o których mowa w art. 1 ust. 1 pkt 1;

2) dane osobowe są przekazywane administratorowi w państwie trzecim lub organizacji międzynarodowej, który jest podmiotem właściwym do realizacji celów, o których mowa w art. 1 ust. 1 pkt 1, z zastrzeżeniem art. 18e ust. 1;
3) państwo członkowskie Unii Europejskiej, które przekazało dane osobowe, wyraziło uprzednią zgodę na ich przekazanie do państwa trzeciego lub organizacji międzynarodowej, a w przypadku dalszego przekazania tych danych do kolejnego państwa trzeciego lub organizacji międzynarodowej właściwy organ ścigania, który dokonał pierwotnego przekazania, lub inny właściwy organ ścigania tego samego państwa członkowskiego Unii Europejskiej zezwala na dalsze przekazanie po należytym uwzględnieniu całokształtu sprawy;
4) Komisja Europejska w przypadku, o którym mowa w art. 18b ust. 1, uznała, że państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim, lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych osobowych;
5) w razie braku decyzji Komisji, o której mowa w art. 18b ust. 1:
   a) zostały zapewnione lub istnieją odpowiednie zabezpieczenia zgodnie z art. 18c – w przypadku gdy nie zostały spełnione warunki, o których mowa w pkt 4,
   b) ma zastosowanie wyjątek w szczególnych sytuacjach zgodnie z art. 18d – w przypadku gdy nie zostały spełnione warunki, o których mowa w pkt 5 lit. a.

2. Przekazanie danych osobowych bez uprzedniej zgody innego państwa członkowskiego Unii Europejskiej, o której mowa w ust. 1 pkt 3, jest dozwolone wyłącznie wtedy, gdy takiej uprzedniej zgody nie da się uzyskać w odpowiednim terminie, a przekazanie jest:

1) niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego w państwie członkowskim Unii Europejskiej lub państwie trzecim lub
2) ma istotne znaczenie dla ważnych interesów państwa członkowskiego Unii Europejskiej.

3. W przypadku zastosowania przepisu ust. 2 państwo członkowskie Unii Europejskiej odpowiadające za wydanie uprzedniej zgody zostaje powiadomione bez zbędnej zwłoki.

4. Podmiot uprawniony lub punkt kontaktowy mogą, o ile przepisy odrębne nie stanowią inaczej, zezwolić organowi ścigania państwa członkowskiego Unii Europejskiej na przekazanie do państwa trzeciego lub organizacji międzynarodowej danych osobowych, uprzednio przekazanych temu organowi przez podmiot uprawniony lub punkt kontaktowy, o ile przekazał on dane osobowe, realizując zadanie określone w art. 5 pkt 1. Jeżeli organ ścigania państwa członkowskiego Unii Europejskiej wystąpił do podmiotu uprawnionego lub punktu kontaktowego o zgodę na dalsze przekazanie danych osobowych uprzednio od nich otrzymanych do kolejnego państwa trzeciego lub organizacji międzynarodowej, organ uprawniony lub punkt kontaktowy może zezwolić na to dalsze przekazanie po należytym uwzględnieniu całokształtu sprawy, w tym:

1) wagi czynu zabronionego;
2) celu, w którym dane osobowe zostały pierwotnie przekazane;
3) stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których dane osobowe są dalej przekazywane.

Art. 18b. 1. Dane osobowe mogą zostać przekazane do państwa trzeciego, terytorium lub przynajmniej jednego sektora w tym państwie trzecim, lub danej organizacji międzynarodowej – o ile Komisja Europejska w drodze decyzji uznała, iż państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub dana organizacja międzynarodowa zapewnia odpowiedni stopień ochrony danych osobowych.

2. Wydanie przez Komisję Europejską decyzji stwierdzającej, że państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony danych osobowych – nie wpływa na przekazywanie danych osobowych do danego państwa trzeciego, terytorium lub jednego lub więcej określonych sektorów w tym państwie trzecim, lub do danej organizacji międzynarodowej na mocy art. 18c i art. 18d.

Art. 18c. 1. W przypadku braku decyzji Komisji Europejskiej, o której mowa w art. 18b ust. 1, dane osobowe mogą zostać przekazane do państwa trzeciego lub organizacji międzynarodowej, jeżeli przepisy prawa przewidują odpowiednie zabezpieczenia ochrony danych osobowych.

2. W przypadku braku prawnie wiążącego aktu, o którym mowa w ust. 1, dane osobowe mogą zostać przekazane do państwa trzeciego lub organizacji międzynarodowej, jeżeli administrator stwierdził, po przeanalizowaniu wszystkich

okoliczności związanych z przekazaniem danych osobowych, że to państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni poziom zabezpieczenia ochrony danych osobowych, w szczególności poufności przekazanych danych, celu, w którym dane zostały przekazane, lub sposobu ich wykorzystania, tak aby nie zostały one użyte do wydania orzeczenia lub wykonania kary śmierci, lub innego rodzaju okrutnego lub nieludzkiego traktowania lub karania.

3. Administrator dokumentuje fakt przekazania danych osobowych w przypadkach, o których mowa w ust. 2, oraz niezwłocznie informuje Prezesa Urzędu Ochrony Danych Osobowych o tym fakcie.

4. Podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, dokumentują, w sposób określony w ust. 5, fakt przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, które zostały przez administratora uznane, na podstawie ust. 2, za zapewniające odpowiedni poziom zabezpieczenia ochrony danych osobowych.

5. Podmiot uprawniony lub punkt kontaktowy, o ile realizował zadanie określone w art. 5 pkt 1, udostępnia Prezesowi Urzędu Ochrony Danych Osobowych, na każde jego żądanie, dokumentację obejmującą:

1) datę i godzinę przekazania;
2) informacje o właściwym organie odbierającym;
3) uzasadnienie przekazania;
4) wyliczenie danych osobowych, jakie zostały przekazane.

6. Prezes Urzędu Ochrony Danych Osobowych współpracuje z podmiotami uprawnionymi i punktem kontaktowym w celu prawidłowej realizacji obowiązku zawartego w ust. 2.

Art. 18d. 1. W przypadku braku decyzji Komisji Europejskiej, o której mowa w art. 18b ust. 1, oraz braku odpowiednich zabezpieczeń, o których mowa w art. 18c ust. 1 i 2, dane osobowe lub określona ich kategoria mogą zostać przekazane do państwa trzeciego lub organizacji międzynarodowej wyłącznie pod warunkiem, że przekazanie jest niezbędne:

1) w celu ochrony życia lub zdrowia osoby, której dane dotyczą, lub innej osoby;
2) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą, jeżeli przepisy odrębne tak stanowią;

3) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego Unii Europejskiej lub państwa trzeciego;
4) w indywidualnym przypadku do celów, o których mowa w art. 1 ust. 1 pkt 1;
5) w indywidualnym przypadku, dla ustalenia, dochodzenia lub obrony roszczeń w związku z celami określonymi w art. 1 ust. 1 pkt 1.

2. Danych osobowych nie przekazuje się, jeżeli podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, stwierdziły, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem, o którym mowa w ust. 1 pkt 4 i 5.

3. Podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, dokumentują, w sposób określony w ust. 4, fakt przekazania danych osobowych na podstawie ust. 1 do państwa trzeciego lub organizacji międzynarodowej.

4. Podmiot uprawniony lub punkt kontaktowy, o ile realizował zadanie określone w art. 5 pkt 1, udostępnia Prezesowi Urzędu Ochrony Danych Osobowych, na każde jego żądanie, dokumentację obejmującą:

1) datę i godzinę przekazania;
2) informacje o właściwym organie odbierającym;
3) uzasadnienie przekazania;
4) wyliczenie danych osobowych, jakie zostały przekazane.

Art. 18e. 1. Na zasadzie wyjątku od art. 18a ust. 1 pkt 2 oraz z zastrzeżeniem wyjątków przewidzianych w umowach międzynarodowych dotyczących współpracy policyjnej zawartych z państwami trzecimi, dane osobowe w indywidualnych i konkretnych przypadkach mogą zostać przekazane bezpośrednio odbiorcom mającym siedzibę w państwach trzecich jedynie wówczas, gdy spełnione zostały łącznie następujące warunki:

1) przekazanie jest niezbędne do wykonania prawnie określonego zadania podmiotu uprawnionego do celów, o których mowa w art. 1 ust. 1 pkt 1;
2) podmiot uprawniony stwierdza, że podstawowe prawa i wolności danej osoby, której dane dotyczą, nie są nadrzędne wobec interesu publicznego przemawiającego za przedmiotowym przekazaniem;
3) podmiot uprawniony uznaje, że przekazanie organowi ścigania państwa trzeciego do celów, o których mowa w art. 1 ust. 1 pkt 1, byłoby nieskuteczne lub

niewłaściwe, w szczególności z uwagi na niemożność zachowania odpowiedniego terminu;

4) organ ścigania państwa trzeciego zostaje o tym poinformowany bez zbędnej zwłoki, chyba że byłoby to nieskuteczne lub niewłaściwe;

5) podmiot uprawniony informuje odbiorcę o konkretnym celu, w którym dane osobowe mają być wyłącznie przetwarzane przez odbiorcę, pod warunkiem że takie przetwarzanie jest niezbędne.

2. Podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, dokumentują fakt przekazania danych osobowych na podstawie ust. 1 oraz niezwłocznie informują Prezesa Urzędu Ochrony Danych Osobowych o tym fakcie.

3. Podmiot uprawniony lub punkt kontaktowy, o ile realizował zadanie określone w art. 5 pkt 1, udostępnia Prezesowi Urzędu Ochrony Danych Osobowych, na każde jego żądanie, dokumentację obejmującą:

1) datę i godzinę przekazania;

2) informacje o właściwym organie odbierającym;

3) uzasadnienie przekazania;

4) wyliczenie danych osobowych, jakie zostały przekazane.

Art. 18f. Do wymiany informacji z państwami trzecimi lub organizacjami międzynarodowymi stosuje się odpowiednio przepisy art. 11 ust. 1 pkt 2 i ust. 2, art. 12, z wyłączeniem ust. 1a, art. 13, art. 14, art. 16 i art. 17.”;

15) art. 19 otrzymuje brzmienie:

„Art. 19. 1. Podmioty uprawnione mogą wymieniać dane osobowe z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, po uprzednim zweryfikowaniu ich prawidłowości, aktualności i kompletności oraz w sposób umożliwiający podmiotom, o których mowa w art. 1 ust. 1 pkt 1, dokonanie oceny tych danych w tym zakresie.

2. Podmiot uprawniony, który otrzymał dane osobowe od podmiotów, o których mowa w art. 1 ust. 1 pkt 1, bez wniosku, dokonuje niezwłocznie weryfikacji tych danych w zakresie ich przydatności do realizacji celu, w którym dane zostały przekazane.

3. Podmiot uprawniony lub punkt kontaktowy, który przekazał nieprawdziwe, niekompletne, nieaktualne lub niezupełne dane osobowe albo przekazał te dane z naruszeniem przepisów ustawy, jest obowiązany, bez zbędnej zwłoki, poinformować o tym podmioty, o których mowa w art. 1 ust. 1 pkt 1, oraz sprostować, uzupełnić lub

uaktualnić te dane, przekazując dane właściwe, albo, w zależności od okoliczności, o których mowa w art. 21 ust. 1, dane te usunąć.”;

16) w art. 20:

a) ust. 1 i 2 otrzymują brzmienie:

„1. Dane osobowe, uzyskane w wyniku wymiany z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, podmiot uprawniony przechowuje przez okres niezbędny do realizacji celu, w jakim te dane zostały uzyskane, lub przez okres niezbędny do wykrywania i ścigania sprawców przestępstw lub przestępstw skarbowych oraz zapobiegania przestępczości lub jej zwalczania, zgodnie z terminami oraz zasadami przetwarzania danych w zbiorach danych administrowanych przez dany podmiot uprawniony.

2. Podmioty uprawnione dokonują weryfikacji zgromadzonych danych osobowych i usuwają dane zbędne albo dokonują ich pseudonimizacji.”,

b) uchyla się ust. 3 i 4,

c) dodaje się ust. 5 w brzmieniu:

„5. Dane osobowe, wymieniane z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, oraz podmiotami uprawnionymi, punkt kontaktowy przechowuje i przetwarza przez okres niezbędny do realizacji zadania, o którym mowa w art. 5 pkt 5.”;

17) w art. 21 ust. 1 otrzymuje brzmienie:

„1. Jeżeli podmiot, o którym mowa w art. 1 ust. 1 pkt 1, przy wymianie danych osobowych określił termin ich przechowywania, po upływie którego wymagane jest ich usunięcie lub zweryfikowanie, podmiot uprawniony, który te dane otrzymał i przechowuje, ma obowiązek zachowania takiego terminu.”;

18) art. 22 otrzymuje brzmienie:

„Art. 22. Jeżeli podmiot, o którym mowa w art. 1 ust. 1 pkt 1, przy wymianie danych osobowych określił ograniczenia dotyczące przetwarzania tych danych wynikające z prawa krajowego tego państwa, podmiot uprawniony, który te dane otrzymał i przechowuje, ma obowiązek uwzględnić takie ograniczenia.”;

19) w art. 23 ust. 1 otrzymuje brzmienie:

„1. Podmioty uprawnione, które przekazały lub udostępniły dane osobowe podmiotowi, o którym mowa w art. 1 ust. 1 pkt 1, albo otrzymały takie dane od tego podmiotu, odnotowują lub dokumentują fakt takiego przekazania, udostępnienia lub

otrzymania w celu weryfikacji legalności przetwarzanych danych, ich integralności oraz zapewnienia ich bezpieczeństwa.”;

20) uchyla się art. 24 i art. 25;

21) w art. 26:

a) ust. 1 otrzymuje brzmienie:

„1. W sprawach nieuregulowanych w niniejszej ustawie stosuje się przepisy ustawy z dnia …. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …).”,

b) uchyla się ust. 2.

Art. 86. W ustawie z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym (Dz. U. z 2018 r. poz. 1466 i 1479) w art. 2 w ust. 2 w pkt 10 kropkę zastępuje się średnikiem i dodaje się pkt 11 w brzmieniu:

„11) informatycznych nośników danych wykorzystywanych do przetwarzania danych osobowych, o których mowa w ustawie z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …).”.

Art. 87. W ustawie z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5, 1000, 1443 i 1669) po art. 191 dodaje się art. 191a w brzmieniu:

„Art. 191a. § 1. Nadzór nad przetwarzaniem danych osobowych w ramach realizacji zadań określonych w art. 2, których administratorami są powszechne jednostki organizacyjne prokuratury zgodnie z art. 13 § 6, wykonują:

1) w zakresie działalności prokuratury rejonowej – prokurator okręgowy;
2) w zakresie działalności prokuratury okręgowej – prokurator regionalny;
3) w zakresie działalności prokuratury regionalnej i Prokuratury Krajowej – Prokurator Krajowy.

§ 2. W ramach nadzoru, o którym mowa w § 1, właściwe organy:

1) rozpatrują skargi osób, których dane osobowe są przetwarzane niezgodnie z prawem;
2) podejmują działania mające na celu upowszechnianie wśród nadzorowanych administratorów i podmiotów przetwarzających wiedzy o obowiązkach

wynikających z ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. ...);

3) współpracują wzajemnie oraz z organami sprawującymi nadzór nad przetwarzaniem danych osobowych w ramach postępowań prowadzonych przez sądy i trybunały z organami nadzorczymi w rozumieniu art. 51 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), jak też współpracują między sobą, w tym dzielą się informacjami, oraz świadczą z tymi organami i między sobą wzajemną pomoc w celu zapewnienia spójnego stosowania przepisów ustawy z dnia …. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

§ 3. Organy, o których mowa w § 1, są uprawnione do:

1) nakazywania administratorowi lub podmiotowi przetwarzającemu albo ich przedstawicielom dostarczenia wszelkich informacji potrzebnych do realizacji zadań tego organu;
2) zawiadamiania administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia przepisów ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
3) uzyskiwania od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych oraz informacji niezbędnych organowi nadzorczemu do realizacji jego zadań;
4) uzyskiwania dostępu do pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych;
5) wydawania ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów ustawy z dnia …. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
6) udzielania upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;

7) wzywania administratora lub podmiotu przetwarzającego do dostosowania operacji przetwarzania danych do przepisów ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

§ 4. Do przyjmowania i rozpatrywania skarg, o których mowa w § 2 pkt 1, stosuje się odpowiednio przepisy działu VI.”.

Art. 88. W ustawie z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (Dz. U. z 2018 r. poz. 410 i 1000) art. 9 otrzymuje brzmienie:

„Art. 9. Do danych osobowych zgromadzonych w systemie zgłaszania stosuje się przepisy ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. ...).”.

Art. 89. W ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2018 r. poz. 508, z późn. zm.[27)]) wprowadza się następujące zmiany:

1) w art. 35 dodaje się ust. 5 w brzmieniu:

„5. Do danych zgromadzonych oraz przetwarzanych w CRDP w związku z realizacją zadań związanych z rozpoznawaniem, zapobieganiem, wykrywaniem i zwalczaniem czynów zabronionych stosuje się przepisy ustawy z dnia … … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …).”;

2) w art. 47 w ust. 1 w pkt 2:

a) po lit. b dodaje się lit. ba w brzmieniu:

„ba) ustawie z dnia 21 listopada 1996 r. o muzeach,”,

b) po lit. d dodaje się lit. da w brzmieniu:

„da) ustawie z dnia 27 czerwca 1997 r. o bibliotekach,”,

c) dodaje się lit. m w brzmieniu:

„m) ustawie z dnia 9 marca 2017 r. o systemie monitorowania drogowego i kolejowego przewozu towarów;”;

3) po art. 47 dodaje się art. 47a w brzmieniu:

„Art. 47a. Organy KAS w celu realizacji ustawowych zadań są uprawnione do wymiany informacji, w tym danych osobowych, z organami ścigania państw

---

27) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 723, 1000, 1039, 1499, 1544, 1577 i 1654.

członkowskich Unii Europejskiej zajmującymi się zapobieganiem i zwalczaniem przestępczości oraz innymi organizacjami międzynarodowymi na zasadach i warunkach określonych w przepisach odrębnych, prawie Unii Europejskiej i umowach międzynarodowych.”;

4) po art. 52 dodaje się art. 52a–52c w brzmieniu:

„Art. 52a. 1. Przetwarzanie danych osobowych przez organy KAS w celu, o którym mowa w art. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na zasadach określonych w tej ustawie.

2. Danych osobowych, o których mowa w art. 14 ust. 1 ustawy, o której mowa w ust. 1, nie gromadzi się, w przypadku gdy nie mają one przydatności wykrywczej lub dowodowej.

Art. 52b. 1. Dane osobowe zbierane i przetwarzane przez KAS na podstawie rozporządzenia 2016/679 mogą być przetwarzane przez organy KAS również dla celów określonych w art. 1 pkt 1 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

2. Dane osobowe przetwarzane przez KAS dla celów określonych w art. 1 pkt 1 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości mogą być przetwarzane przez organy KAS również dla innych celów.

Art. 52c. Organy KAS mogą przetwarzać dane osobowe bez wiedzy i zgody osób, których dane dotyczą.”;

5) po art. 126 dodaje się art. 126a w brzmieniu:

„Art. 126a. Przetwarzanie danych osobowych na podstawie niniejszej ustawy przez właściwe organy KAS w celu realizowania zadań oraz wykonywania czynności, o których mowa w art. 113 ust. 1, odbywa się na zasadach określonych w ustawie z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, prawie Unii Europejskiej oraz postanowieniach umów międzynarodowych.”.

Art. 90. W ustawie z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz. U. poz. 2072) po art. 35 dodaje się art. 35a i art. 35b w brzmieniu:

„Art. 35a. 1. Trybunał jest administratorem danych osobowych przetwarzanych w ramach prowadzonych przez niego postępowań.

2. Do przetwarzania danych osobowych w postępowaniach prowadzonych przez Trybunał przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 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, z późn. zm.[28)]), zwanego dalej „rozporządzeniem 2016/679", nie stosuje się.

3. W związku z przetwarzaniem danych osobowych w postępowaniach prowadzonych przez Trybunał wykonanie obowiązków, o których mowa w art. 13 rozporządzenia 2016/679, następuje przez umieszczenie informacji określonych w art. 13 rozporządzenia 2016/679 na stronie podmiotowej Biuletynu Informacji Publicznej oraz w widocznym miejscu w budynku Trybunału.

Art. 35b. 1. Nadzór nad przetwarzaniem danych osobowych przez Trybunał w ramach prowadzonych przez niego postępowań wykonuje Krajowa Rada Sądownictwa.

2. Do nadzoru, o którym mowa w ust. 1, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych stosuje się odpowiednio.".

Art. 91. W ustawie z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami (Dz. U. poz. 648 oraz z 2018 r. poz. 723 i 1499) po art. 6 dodaje się art. 6a w brzmieniu:

„Art. 6a. Do udostępniania informacji otrzymanych na podstawie ustawy oraz umów o unikaniu podwójnego opodatkowania, innych ratyfikowanych umów, których stroną jest Rzeczpospolita Polska, oraz innych umów międzynarodowych, których stroną jest Unia Europejska, a także porozumień zawartych na podstawie tych umów,

---

[28)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.5.2018, str. 2.

nie stosuje się przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości w zakresie, w jakim jest to niezgodne z postanowieniami tych umów lub porozumień lub przepisami ustawy.”.

Art. 92. W ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2017 r. poz. 1566, z późn. zm.[29)]) po art. 341 dodaje się art. 341a w brzmieniu:

„Art. 341a. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), jest minister właściwy do spraw gospodarki wodnej lub organ wykonujący kontrolę.”.

Art. 93. W ustawie z dnia 8 grudnia 2017 r. o Sądzie Najwyższym (Dz. U. z 2018 r. poz. 5, z późn. zm.[30)]) wprowadza się następujące zmiany:

1) art. 8 otrzymuje brzmienie:

„Art. 8. Sąd Najwyższy niezwłocznie publikuje wydane przez siebie orzeczenie, a po sporządzeniu jego uzasadnienia – również uzasadnienie orzeczenia, w Biuletynie Informacji Publicznej na stronie podmiotowej Sądu Najwyższego.”;

2) po art. 9 dodaje się art. 9a w brzmieniu:

„Art. 9a. § 1. Sąd Najwyższy jest administratorem danych osobowych przetwarzanych w postępowaniach sądowych.

§ 2. Do przetwarzania danych osobowych w postępowaniach sądowych przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 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, z późn. zm.[31)]), zwanego dalej „rozporządzeniem 2016/679”, nie stosuje się.

§ 3. W związku z przetwarzaniem danych osobowych w postępowaniach sądowych wykonanie obowiązków, o których mowa w art. 13 rozporządzenia 2016/679, następuje przez umieszczenie informacji określonych w art. 13 rozporządzenia 2016/679 na

---

29) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 710, 1479, 1669 i 1722.
30) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 771, 847, 848, 1045 i 1443.
31) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

stronie podmiotowej Biuletynu Informacji Publicznej oraz w widocznym miejscu w budynku Sądu Najwyższego.”;

3) po art. 97 dodaje się art. 97a w brzmieniu:

„Art. 97a. § 1. Nadzór nad przetwarzaniem danych osobowych w postępowaniach sądowych wykonuje Krajowa Rada Sądownictwa.

§ 2. Do nadzoru, o którym mowa w § 1, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych stosuje się odpowiednio.”.

Art. 94. W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138, 650, 730, 1544, 1562 i 1669) wprowadza się następujące zmiany:

1) w art. 51 uchyla się zdanie drugie;

2) w art. 56:

a) w ust. 6 pkt 1 otrzymuje brzmienie:

„1) dane osobowe, o których mowa w art. 14 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …);”,

b) w ust. 8 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Dane osobowe, o których mowa w ust. 2 i 3 oraz art. 40 ust. 1, z wyjątkiem danych osobowych, o których mowa w ust. 6 pkt 1, SOP może przetwarzać:”,

c) uchyla się ust. 9 i 11;

3) w art. 59 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„W celu realizacji zadań, o których mowa w art. 19 ust. 1 pkt 2, SOP może uzyskiwać dane:”;

4) uchyla się art. 60;

5) art. 61 otrzymuje brzmienie:

„Art. 61. Administratorem danych osobowych przetwarzanych przez SOP jest Komendant SOP.”;

6) po art. 70 dodaje się art. 70a w brzmieniu:

„Art. 70a. 1. SOP jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w SOP, przenoszenia do służby w SOP oraz w zakresie wynikającym z przebiegu stosunku służbowego funkcjonariuszy SOP, także po jego ustaniu, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia (UE)

2016/679, z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 tego rozporządzenia w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności.”.

Art. 95. W ustawie z dnia 10 stycznia 2018 r. o szczególnych rozwiązaniach związanych z organizacją w Rzeczypospolitej Polskiej sesji Konferencji Stron Ramowej konwencji Narodów Zjednoczonych w sprawie zmian klimatu (Dz. U. poz. 319, 730, 1495 i 1637) wprowadza się następujące zmiany:

1) w art. 17:

a) w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„W celu zapewnienia bezpieczeństwa i porządku publicznego podczas Konferencji COP24, a także w celu zapobieżenia popełnianiu przestępstw i wykroczeń oraz wykrywania i ścigania ich sprawców, Policja i Służba Ochrony Państwa mogą przetwarzać informacje, w tym dane osobowe:”;

b) ust. 2 otrzymuje brzmienie;

„2. Do zakresu informacji, o których mowa w ust. 1, stosuje się odpowiednio przepisy art. 20 ust. 2b ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.[32)]) oraz art. 56 ust. 6 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138, 650, 730, 1544, 1562 i 1669).”;

2) w art. 18:

a) ust. 1 otrzymuje brzmienie:

„1. Udostępnienie przez Policję oraz Służbę Ochrony Państwa informacji, o których mowa w art. 17 ust. 1, w celu zapewnienia bezpieczeństwa i porządku publicznego podczas Konferencji COP24, a także w celu zapobieżenia popełnianiu przestępstw i wykroczeń oraz wykrywania i ścigania ich sprawców, organom,

---

[32)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544 i 1669.

służbom i instytucjom państwowym, w tym również odpowiednio zagranicznym i międzynarodowym, odbywa się na zasadach określonych odpowiednio w przepisach ustawy z dnia 6 kwietnia 1990 r. o Policji, ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. ...), ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2018 r. poz. 484 i ...), ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, 650, 1000, 1083 i 1669 oraz z 2017 r. poz. 935), a także w umowach międzynarodowych, których Rzeczpospolita Polska jest stroną.”,

b) w ust. 2 zdanie pierwsze otrzymuje brzmienie:

„Policja i Służba Ochrony Państwa udostępniają informacje, o których mowa w art. 17 ust. 1 pkt 2, po uzyskaniu zgody organu, służby lub instytucji, które te informacje uzyskały lub przetwarzały.”,

c) w ust. 3 pkt 1 i 2 otrzymują brzmienie:

„1) udostępnianie tych informacji mogłoby utrudnić lub uniemożliwić realizację zadań Policji lub Służby Ochrony Państwa lub

2) Policja lub Służba Ochrony Państwa nie uzyskała zgody, o której mowa w ust. 2.”;

3) w art. 19:

a) w ust. 1 po wyrazie „Policji” dodaje się wyrazy „lub Służby Ochrony Państwa”,

b) ust. 2 otrzymuje brzmienie:

„2. Informacje, o których mowa w art. 17 ust. 1, usuwa się ze zbiorów danych osobowych, których administratorem jest Komendant Główny Policji lub Komendant Służby Ochrony Państwa, z wyjątkiem informacji, o których mowa odpowiednio w art. 20 ust. 2a ustawy z dnia 6 kwietnia 1990 r. o Policji i w art. 56 ust. 2 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, przetwarzanych na potrzeby toczących się postępowań, po upływie terminu, o którym mowa w art. 17 ust. 1.”;

4) w art. 20 po wyrazie „Policji” dodaje się przecinek i wyrazy „Służby Ochrony Państwa”.

Art. 96. W ustawie z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej (Dz. U. poz. 729 i 1669) wprowadza się następujące zmiany:

1) w art. 4

a) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Administratorem danych osobowych, o których mowa w ust. 2 pkt 2, jest Komendant Straży Marszałkowskiej.”;

b) uchyla się ust. 4;

2) po art. 19 dodaje się art. 19a w brzmieniu:

„Art. 19a. 1. Straż Marszałkowska jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w Straży Marszałkowskiej, przenoszenia do służby w Straży Marszałkowskiej oraz w zakresie wynikającym z przebiegu stosunku służbowego funkcjonariuszy Straży Marszałkowskiej, także po jego ustaniu, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia (UE) 2016/679, z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 tego rozporządzenia w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności.”.

Art. 97. W ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. poz. 723, 1075 i 1499) wprowadza się następujące zmiany:

1) w art. 96 ust. 3 otrzymuje brzmienie:

„3. Dane, o których mowa w art. 14 ustawy z dnia … o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), mogą być zbierane i wykorzystywane oraz przetwarzane przez Generalnego Inspektora wyłącznie w przypadku, gdy jest to niezbędne ze względu na zakres wykonywanych zadań lub czynności.”;

2) w art. 97:

a) uchyla się ust. 1–5,

b) ust. 6 i 7 otrzymują brzmienie:

„6. Kierownik komórki organizacyjnej, o której mowa w art. 12 ust. 2, któremu inspektor ochrony danych wydał pisemne polecenie usunięcia stwierdzonych uchybień, informuje Generalnego Inspektora, w terminie 7 dni od dnia wydania tego polecenia, o jego wykonaniu lub przyczynie jego niewykonania.

7. W przypadku naruszenia przepisów ustawy lub przepisów o ochronie danych osobowych inspektor ochrony danych podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Generalnego Inspektora oraz ministra właściwego do spraw finansów publicznych.”;

3) uchyla się ust. 8.

Art. 98. W ustawie z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. poz. 894) wprowadza się następujące zmiany:

1) w art. 9 w ust. 2 pkt 5 otrzymuje brzmienie:

„5) pouczenie o prawie do złożenia wniosku o udzielenie informacji o przysługujących mu prawach lub złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych w zakresie przetwarzania danych osobowych pasażera w związku z przetwarzaniem danych PNR.” ;

2) w art. 36 po pkt 4 dodaje się pkt 4a w brzmieniu:

„4a) Komendant Służby Ochrony Państwa;”;

3) w art. 53:

a) w ust. 1 pkt 3 otrzymuje brzmienie:

„3) państwo trzecie zapewnia odpowiedni poziom ochrony przekazywanych danych określony w art. 18b–18d ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2018 r. poz. 484 i ...);”,

b) uchyla się ust. 2;

4) w art. 59 w ust. 1 pkt 2 otrzymuje brzmienie:

„2) sprawuje nadzór nad zgodnością przetwarzania danych PNR przez JTP z przepisami niniejszej ustawy oraz ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …);”;

5) w art. 62 w ust. 3 pkt 2 otrzymuje brzmienie:

„2) sprawdza zgodność przetwarzania danych PNR z prawem, prowadzi postępowania i wykonuje inne czynności, zgodnie z ustawą z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z własnej inicjatywy lub na podstawie zażalenia osoby, której dane PNR są przetwarzane.”;

6) w art. 63 ust. 3 otrzymuje brzmienie:

„3. Kontrola, o której mowa w ust. 1, jest sprawowana zgodnie z przepisami ustawy z dnia ... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.”;

7) użyte w art. 59 w ust. 1 w pkt 3 i w ust. 2 w pkt 4 i 5, w art. 61, w art. 62 oraz w art. 63 w ust. 1 i 2, w różnym przypadku wyrazy „Generalny Inspektor Ochrony Danych Osobowych” zastępuje się użytymi w odpowiednim przypadku wyrazami „Prezes Urzędu Ochrony Danych Osobowych”.

Rozdział 10

Przepisy przejściowe, dostosowujące i końcowe

Art. 99. 1. Osoba pełniąca w dniu wejścia w życie niniejszej ustawy funkcję administratora bezpieczeństwa informacji, o którym mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723), staje się inspektorem ochrony danych i pełni swoją funkcję nie dłużej jednak niż 3 miesiące od dnia wejścia w życie niniejszej ustawy, 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. 46.

2. Osoba, która stała się inspektorem ochrony danych na podstawie ust. 1, pełni swoją funkcję także po upływie 3 miesięcy od dnia wejścia w życie niniejszej ustawy, jeżeli do tego dnia administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o jej wyznaczeniu, w sposób określony w art. 46.

3. Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał administratora bezpieczeństwa informacji, o którym mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jest obowiązany do wyznaczenia inspektora ochrony danych i zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu, w terminie 1 miesiąca od dnia wejścia w życie niniejszej ustawy.

Art. 100. 1. Do kontroli wszczętych na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

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

Art. 101. 1. Postępowania prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych, wszczęte i niezakończone przed dniem wejścia w życie niniejszej ustawy, prowadzone są na podstawie przepisów dotychczasowych.

2. Czynności dokonane w postępowaniach, o których mowa w ust. 1, pozostają skuteczne, o ile zostały dokonane zgodnie z przepisami obowiązującymi w czasie ich dokonywania.

3. W przypadku wniesienia przed dniem wejścia w życie niniejszej ustawy, na podstawie art. 21 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wniosku o ponowne rozpatrzenie sprawy, będące w toku postępowanie wszczęte tym wnioskiem umarza się z mocy prawa z dniem wejścia w życie niniejszej ustawy.

4. Stronę, która zainicjowała postępowanie, o którym mowa w ust. 3, organ poucza o prawie złożenia do sądu administracyjnego skargi na decyzję, od której strona złożyła wniosek o ponowne rozpatrzenie sprawy.

5. Termin na wniesienie skargi w przypadku, o którym mowa w ust. 4, wynosi 3 miesiące od dnia doręczenia pouczenia. Do czasu upływu tego terminu decyzja, od której strona złożyła wniosek o ponowne rozpatrzenie sprawy, nie podlega wykonaniu.

Art. 102. Podmiot, do którego przed dniem wejścia w życie ustawy zostało skierowane wystąpienie lub wniosek, o których mowa w art. 19a ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jest obowiązany przekazać Prezesowi Urzędu Ochrony Danych Osobowych odpowiedź na wystąpienie lub wniosek, na piśmie, w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

Art. 103. 1. W terminie 1 roku od dnia wejścia w życie ustawy administrator dostosowuje zasady przetwarzania danych osobowych do środków technicznych i organizacyjnych, o których mowa w art. 39.

2. Jeżeli wymaga to niewspółmiernie dużego wysiłku lub nakładów, administrator może dostosować zautomatyzowane systemy przetwarzania danych osobowych do środków

technicznych i organizacyjnych, w terminie dłuższym niż wskazanym w ust. 1, nie później jednak niż do dnia 6 maja 2023 r.

3. Dotychczasowe rozstrzygnięcia określające zasady udostępniania informacji i danych osobowych z Centralnej Bazy Danych Osób Pozbawionych Wolności, za pośrednictwem systemu teleinformatycznego, zachowują moc do dnia wejścia w życie decyzji wydanych na podstawie art. 25d ust. 1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, dodanego niniejszą ustawą, nie dłużej jednak niż przez okres 2 lat od dnia wejścia w życie niniejszej ustawy.

4. Dostosowanie zasad przetwarzania informacji i danych osobowych w zbiorach danych utworzonych przed dniem wejścia w życie niniejszej ustawy do wymogów, o których mowa w art. 19, art. 20 i art. 36, nastąpi nie później niż do dnia 6 maja 2023 r.

Art. 104. Wydane przed dniem wejścia w życie ustawy upoważnienia do przetwarzania danych osobowych zachowują moc przez okres 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 105. Zgody wydane przez służby, instytucje państwowe oraz organy władzy publicznej na udostępnianie za pomocą urządzeń telekomunikacyjnych lub w drodze teletransmisji informacji, w tym danych osobowych, jednostkom organizacyjnym Policji, jednostkom organizacyjnym Straży Granicznej, Służbie Ochrony Państwa oraz organom Krajowej Administracji Skarbowej zachowują swoją moc, z zastrzeżeniem art. 103 ust. 3.

Art. 106. Dotychczasowe przepisy wykonawcze wydane na podstawie:

1) art. 15 ust. 8 i art. 20 ust. 19 ustawy zmienianej w art. 58,
2) art. 10a ust. 8 i art. 11 ust. 2 ustawy zmienianej w art. 59,
3) art. 25 ust. 3 ustawy zmienianej w art. 80,
4) art. 42 ust. 6 ustawy zmienianej w art. 81,
5) art. 24a ust. 5 ustawy zmienianej w art. 82,

6) art. 10 ustawy zmienianej w art. 85

– zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie odpowiednio:

1) art. 15 ust. 8 i art. 20 ust. 1n ustawy zmienianej w art. 58, w brzmieniu nadanym niniejszą ustawą,

2) art. 10a ust. 19 i art. 11 ust. 2 ustawy zmienianej w art. 59, w brzmieniu nadanym niniejszą ustawą,

3) art. 25 ust. 3 ustawy zmienianej w art. 80, w brzmieniu nadanym niniejszą ustawą,

4) art. 42 ust. 6 ustawy zmienianej w art. 81, w brzmieniu nadanym niniejszą ustawą,

5) art. 24a ust. 5 ustawy zmienianej w art. 82, w brzmieniu nadanym niniejszą ustawą,

6) art. 10 ustawy zmienianej w art. 85, w brzmieniu nadanym niniejszą ustawą

– nie dłużej jednak niż przez okres 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 107. 1. Maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy wynosi w:

1) 2018 r. – 310 000 zł;

2) 2019 r. – 1 250 000 zł;

3) 2020 r. – 1 350 000 zł;

4) 2021 r. – 1 380 000 zł;

5) 2022 r. – 1 410 000 zł;

6) 2023 r. – 1 450 000 zł;

7) 2024 r. – 1 490 000 zł;

8) 2025 r. – 1 530 000 zł;

9) 2026 r. – 1 570 000 zł;

10) 2027 r. – 1 610 000 zł;

11) 2028 r. – 1 650 000 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. Ocena za IV kwartał jest dokonywana według stanu na dzień 20 listopada danego roku.

3. W przypadku przekroczenia lub zagrożenia przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków określonego w ust. 1 oraz w przypadku gdy

w okresie od początku roku kalendarzowego do dnia ostatniej oceny, o której mowa w ust. 2, część limitu rocznego przypadającego proporcjonalnie na ten okres zostanie przekroczona co najmniej o 10%, stosuje się mechanizm korygujący polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym niniejszej ustawy.

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

Art. 108. Tracą moc art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziały 4, 5 i 7 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723) zachowane w mocy w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających 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 (Dz. Urz. UE L 119 z 04.05.2016, str. 89) na podstawie art. 175 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).

Art. 109. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem art. 82 pkt 5 w zakresie art. 25c–25h, które wchodzą w życie po upływie roku od dnia ogłoszenia.

UZASADNIENIE

Potrzeba i cel regulacji

Przygotowanie projektu *ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* wynika z konieczności wdrożenia do polskiego porządku prawnego rozwiązań zawartych w dyrektywie 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 04.05.2016, str. 89), zwanej dalej „dyrektywą 2016/680".

Ochrona osób fizycznych w zakresie przetwarzania danych osobowych jest jednym z praw podstawowych. Artykuł 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Dlatego też w celu zapewnienia jednolitych zasad we wszystkich państwach członkowskich Unii Europejskiej oraz wysokiego stopnia ochrony danych osobowych postanowiono na forum europejskim przygotować nowe przepisy w tym zakresie.

Reforma zasad przetwarzania i ochrony danych osobowych w Unii Europejskiej spowodowana była również potrzebą zapewnienia skuteczniejszej ochrony danych osób fizycznych, w związku z szybkim tempem zmian technologicznych powodujących wzrost ilości przetwarzanych danych. Dotychczasowe instrumenty prawne nie były wystarczające, co powodowało, że dane osobowe osób fizycznych narażone były w coraz większym stopniu na zagrożenie.

Dyrektywa 2016/680 oraz kluczowe dla nowej koncepcji ochrony danych osobowych rozporządzenie 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), zwane dalej „rozporządzeniem 2016/679", w sposób

kompleksowy i spójny dla całej Unii Europejskiej regulują zagadnienia ochrony danych.

Ustawodawca europejski celowo wyłączył z zakresu stosowania rozporządzenia 2016/679 przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, regulując te kwestie – ze względu na szczególny charakter takich czynności – w akcie prawnym innej rangi, to jest dyrektywie 2016/680. Dyrektywa bowiem, jako akt prawny zobowiązujący państwa członkowskie do ustanowienia danego porządku prawnego – w przeciwieństwie do rozporządzenia, którego przepisy mają zastosowanie wprost – pozwala na uwzględnienie w przygotowywanych na jej podstawie przepisach różnorodności i odmienności krajowych regulacji w zakresie zapobiegania i zwalczania przestępczości. Przykładem tego rodzaju odmienności jest chociażby dokonane przez polskiego ustawodawcę rozróżnienie czynów karalnych na przestępstwa i wykroczenia, którego źródłem jest ocena szkodliwości społecznej czynów, co w konsekwencji przekłada się na zróżnicowanie dotkliwości sankcji za przestępstwa i wykroczenia. Tego rodzaju systematyka czynów zabronionych nie jest jednak powszechna w Unii Europejskiej.

Istotnym powodem dla przyjęcia takiego rozwiązania była z jednej strony konieczność zapewnienia spójnego, wysokiego stopnia ochrony danych osobowych osób fizycznych, z drugiej zaś ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich umożliwiającej zapewnienie skutecznej współpracy w sprawach karnych i współpracy policyjnej, a także zapewnienie możliwości przekazania danych do państwa trzeciego, pod warunkiem że celem takiego działania będzie ściganie przestępstw przy jednoczesnym zapewnieniu przez państwo trzecie odpowiedniego poziomu ochrony danych.

Jednocześnie dyrektywa do organów właściwych – oprócz organów władzy publicznej takich jak Policja lub inne organy ścigania – zalicza również wszelkie inne organy lub podmioty, którym prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych w celach określonych w dyrektywie 2016/680.

Kryterium celu przetwarzania jest zatem kluczowe dla ustalenia, czy zastosowanie będzie miała dyrektywa 2016/680 czy rozporządzenie 2016/679. Jednocześnie rozporządzenie 2016/679 ma zastosowanie również wtedy, gdy organ lub podmiot zbiera dane osobowe do innych celów, a następnie dalej te dane przetwarza w celu realizacji obowiązku prawnego, któremu podlega.

Brzmienie dyrektywy 2016/680 zostało jednocześnie skorelowane z tekstem ogólnego rozporządzenia o ochronie danych w ten sposób, że oba akty prawne bazują na tych samych zasadach ogólnych. Organy ścigania będą musiały zatem w pełni przestrzegać zasad celowości, adekwatności i legalności. Wyrazem tej tendencji jest również możliwość wyznaczenia tych samych organów nadzorczych.

Dyrektywa 2016/680 reguluje również kwestie wymiany informacji obejmujących dane osobowe między organami ścigania państw członkowskich Unii Europejskiej oraz państwami trzecimi. Obowiązujące dotychczas w tym obszarze regulacje, w postaci uchylanej dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, miały wprawdzie zastosowanie do całości przetwarzania danych osobowych w ramach państwach członkowskich, zarówno w sektorze publicznym, jak i prywatnym. Nie miały jednak zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty", takiej jak działania w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Podobnie uchylana decyzja ramowa Rady 2008/977/WSiSW miała zastosowanie do współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej ograniczony do przetwarzania danych osobowych przesyłanych lub udostępnianych wyłącznie między państwami członkowskimi. Regulacje te okazały się niewystarczające w związku z dynamicznym rozwojem przestępczości o charakterze transgranicznym i międzynarodowym, będącym w znacznej mierze wynikiem postępu technologicznego w zakresie wymiany informacji.

W polskich realiach prawnych kwestie ochrony danych osobowych unormowane były w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz w szeregu innych ustaw regulujących działanie organów ścigania i wymiaru sprawiedliwości, a także innych podmiotów operujących w sferze określonej ramami zakresu podmiotowego dyrektywy 2016/680.

Jednym z głównych założeń nowych regulacji jest utrzymanie równowagi między prawem do prywatności a koniecznością zachowania przez Policję – oraz inne podmioty

funkcjonujące w obszarze zapobiegania i zwalczania przestępczości, w tym ochrony przed zagrożeniami dla bezpieczeństwa i porządku publicznego i zapobiegania takim zagrożeniom – poufności w przetwarzaniu danych w postępowaniach prowadzonych przez właściwe w tym zakresie organy.

Zgodnie z art. 51 ust. 2 Konstytucji RP „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym". Jak wskazuje Rada Legislacyjna działająca przy Prezesie Rady Ministrów, w swojej opinii z dnia 22 czerwca 2018 r., „Pozyskiwanie", „gromadzenie" i „udostępnianie", o których mowa w powyższym przepisie, można uznać za czynności stanowiące „przetwarzanie danych osobowych" w rozumieniu przyjmowanym w ustawodawstwie. Przepis art. 51 ust. 2 Konstytucji oznacza zatem, że przetwarzanie przez organy władzy publicznej „informacji o obywatelu" – to znaczy informacji pozwalającej na zidentyfikowanie osoby – jest dopuszczalne wyłącznie wówczas, gdy jest to konieczne dla realizacji celu uzasadnionego interesem publicznym. Powyższy przepis należy odczytywać w związku z art. 31 ust. 3 Konstytucji, wyrażającym ogólną zasadę proporcjonalności ingerencji państwa w wolności lub prawa jednostek. Kryterium niezbędności, o którym mowa w art. 51 ust. 2 Konstytucji, nie ma natomiast zastosowania do informacji, które nie pozwalają na zidentyfikowanie danej osoby (np. na skutek anonimizacji), lub w sytuacji, gdy zidentyfikowanie osoby jest znacznie utrudnione (np. na skutek pseudonimizacji). W odniesieniu do przetwarzania tego typu informacji swoboda ustawodawcy jest znacznie szersza, co oznacza, że takie informacje mogą być przetwarzane nie tylko w sytuacjach, gdy jest to niezbędne w państwie demokratycznym dla ochrony wartości wymienionych w art. 31 ust. 3 Konstytucji.

Zgodnie z art. 51 ust. 3 zdanie pierwsze Konstytucji „Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych". Z przepisu tego wynika, że jeżeli organ władzy publicznej prowadzi zbiór danych, w których znajdują się informacje dotyczące określonej osoby, to osoba ta ma prawo do żądania wglądu do takiego zbioru. Warunkiem realizacji tego prawa jest możliwość uzyskania informacji o tym, czy w zbiorach prowadzonych przez dany organ władzy publicznej znajduje się jakakolwiek informacja o konkretnej osobie. W przeciwnym razie prawo, o którym mowa w art. 51 ust. 3 Konstytucji, byłoby pozorne. Zgodnie ze zdaniem drugim ww. przepisu „Ograniczenie tego prawa może określić ustawa". Przepis ten należy

odczytywać w związku z ogólną zasadą proporcjonalności (art. 31 ust. 3 Konstytucji), a ponadto jako wzmacniający wymóg zamieszczenia regulacji ograniczającej w ustawie (o tej kwestii będzie jeszcze mowa niżej).

Przepis art. 51 ust. 4 Konstytucji stanowi, że „Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą". Prawo, o którym mowa w tym przepisie, również może podlegać ograniczeniom na zasadach określonych w art. 31 ust. 3 Konstytucji.

Natomiast zgodnie z art. 51 ust. 5 Konstytucji „Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa". Jak wskazuje Rada Legislacyjna jest to kolejny fragment art. 51, w którym podkreślono, że regulacje dotyczące prawa do ochrony danych osobowych powinny znajdować się w ustawie (zob. też art. 51 ust. 1, który mówi, że „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby"). Tak silne wyeksponowanie zasady wyłączności ustawy w kolejnych ustępach art. 51 Konstytucji należy odczytywać w taki sposób, że regulacje dopuszczające przetwarzanie danych osobowych przez organy władzy publicznej, a także ograniczające poszczególne uprawnienia jednostek wskazane w art. 51 powinny znajdować jednoznaczną i precyzyjną podstawę w ustawie. Chodzi nie tylko o formalne zamieszczenie w ustawie przepisu przyznającego organom władzy publicznej kompetencję do przetwarzania danych osobowych, lecz również o odpowiednią jakość tych przepisów. Nie powinny one przyznawać organom władzy publicznej nadmiernej swobody decyzyjnej w omawianym zakresie (np. przez posługiwanie się pojęciami nieostrymi czy klauzulami generalnymi), a w przypadku gdy swoboda taka jest konieczna, powinien istnieć efektywny mechanizm odwoławczy umożliwiający realną kontrolę legalności podejmowanych czynności, dokonywaną przez niezależne organy, w szczególności sądy.

Charakterystyka projektu, wykazanie różnic między stanem aktualnym a projektowanym

Zaproponowane w projekcie rozwiązania stanowią realizacje nałożonego na państwa członkowskie w art. 63 dyrektywy 2016/680 obowiązku transpozycji jej przepisów do krajowego porządku prawnego.

Mając na uwadze powyższe, konieczne było przygotowanie nowego aktu prawnego, który w sposób kompleksowy wdroży do polskiego porządku prawnego rozwiązania

zawarte w dyrektywie 2016/680. Projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i przeciwdziałaniem przestępczości, w części ogólnej (rozdział 1), określa zatem zakres przedmiotowy i podmiotowy tego aktu prawnego, definicję danych osobowych oraz wyjaśnienie innych, stosowanych w ustawie pojęć, przede wszystkim wywodzących się bezpośrednio z dyrektywy 2016/680.

Projektowane przepisy w rozdziale 2 określają zadania organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – który jest co do zasady tożsamy z organem nadzorczym określonym w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, a implementującej do polskiego porządku prawnego rozwiązania wynikające z rozporządzenia 2016/679. Pomimo tego zadania i uprawnienia organu nadzorczego określone w tej części projektowanych przepisów, uwzględniają odmienność celów przetwarzania danych osobowych wynikających z dyrektywy 2016/680. W odniesieniu do prokuratury i sądów organ nadzorczy został określony odrębnie, co znalazło odzwierciedlenie w ustawach kompetencyjnych wymienionych podmiotów.

Projektowane przepisy zawierają również regulacje w zakresie zasad przetwarzania danych osobowych (rozdział 3) oraz praw osób, których dane dotyczą (rozdział 4). Stanowiący istotną część projektowanych przepisów rozdział 5 poświęcony został natomiast kwestiom odnoszącym się do administratora oraz podmiotu przetwarzającego, w tym bardzo istotnym kwestiom odnoszącym się do zabezpieczenia danych osobowych, a także zadaniom i uprawnieniom inspektora ochrony danych osobowych.

Projektowane przepisy regulują również kwestie współpracy Prezesa Urzędu Ochrony Danych Osobowych z organami nadzorczymi w innych państwach Unii Europejskiej (rozdział 6), a także środków ochrony prawnej przysługujących osobom, których dane są przetwarzane (rozdział 7). W rozdziale 8 umieszczone zostały przepisy karne, natomiast w rozdziale 9 przepisy zmieniające, a w rozdziale 10 przepisy przejściowe, dostosowujące i końcowe.

W projekcie wykorzystano także zalecenia sformułowane w opinii dotyczącej wdrażania dyrektywy 2016/680 grupy roboczej artykułu 29 ds. ochronnych danych osobowych (17/EN WP 258 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), a przyjętej 29 listopada 2017 r.

Opis szczegółowych rozwiązań

Zakres przedmiotowy ustawy określony został w art. 1 projektu. W pkt 1 tej jednostki redakcyjnej wskazano, że dane osobowe mogą być przetwarzane w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności. Przez zwalczanie czynów zabronionych należy także rozumieć ściganie czynów zabronionych i wykonywanie kar. Projekt ustawy określa również prawa osób, których dane osobowe są przetwarzane przez właściwe organy oraz środki ochrony prawnej przysługujące tym osobom; sposób prowadzenia nadzoru nad ochroną danych osobowych, z wyłączeniem danych osobowych przetwarzanych przez prokuraturę i sądy; zadania organu nadzorczego oraz formy i sposób ich wykonania; obowiązki administratora i podmiotu przetwarzającego oraz inspektora ochrony danych i tryb jego wyznaczania; sposób zabezpieczenia danych osobowych; tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej oraz odpowiedzialność karną za naruszenie przepisów niniejszej ustawy. Jednocześnie, kierując się wyjaśnieniem zawartym w motywie (80) dyrektywy 2016/680, z zakresu nadzoru określonego w projektowanych przepisach, wyłączono dane osobowe przetwarzane w przez prokuraturę i sądy w toku sprawowania przez nie wymiaru sprawiedliwości.

Dyrektywa 2016/680 posługuje się określeniem bezpieczeństwo publiczne, które na gruncie prawa krajowego używane jest zamiennie lub łącznie i określone jako bezpieczeństwo i porządek publiczny. Porządek publiczny i bezpieczeństwo publiczne stanowią dwie równorzędnie chronione konstytucyjnie wartości. Stanowią one gwarancję praw jednostki do bezpiecznych warunków życia, determinując jednocześnie niezakłócone funkcjonowanie państwa i jego instytucji. Bezpieczeństwo publiczne to stan umożliwiający normalne funkcjonowanie instytucji realizujących zadania, których celem jest ochrona interesów państwa, ochrona życia, zdrowia i mienia ludzi, przy jednoczesnym zapewnieniu poszanowania konstytucyjnie przyznanych praw i wolności jednostki. Natomiast porządek publiczny to przestrzeganie przez obywateli przyjętego wzorca zachowań w miejscach ogólnie dostępnych (publicznych). Oba zdefiniowane wyżej pojęcia pozostają w ścisłym związku, gdyż ochrona bezpieczeństwa publicznego sprzyja budowaniu zasad mających zapewnić ład i porządek. Natomiast egzekwowanie

przez państwo zachowań zgodnych z przyjętymi normami prawnymi i zasadami współżycia społecznego sprzyja utrzymaniu bezpieczeństwa publicznego.

W projekcie nie zdecydowano się na skatalogowanie podmiotów, których ustawa dotyczy. Czynnikiem determinującym stosowanie przepisów projektowanej ustawy będą natomiast kompetencje podmiotu określone w regulacjach prawnych rangi ustawy. Powyższa konstrukcja projektowanych przepisów jest przede wszystkim wynikiem wielości podmiotów funkcjonujących w sferze określonej ramami zakresu podmiotowego dyrektywy 2016/680. Rozwiązanie takie jest przy tym na tyle uniwersalne, że w przypadku utworzenia, likwidacji lub przekształcenia działających w tym obszarze podmiotów, nie będzie skutkowało koniecznością wprowadzania zmian w projektowanych przepisach.

W art. 2 projektu wskazano, że ustawę stosuje się do przetwarzania danych osobowych przez właściwe organy w celach, o których mowa w art. 1 pkt 1, w sposób całkowicie lub częściowo zautomatyzowany lub inny niż zautomatyzowany, w przypadku gdy dane te stanowią lub mają stanowić część zbioru danych. Rozwiązania przyjęte w tym zakresie w ustawie odpowiadają art. 2 ust. 2 dyrektywy.

W art. 3 w pkt 1–2 projektu wskazano wyłączenia w odniesieniu do zakresu przedmiotowego ustawy. Zgodnie z nim przepisów ustawy nie stosuje się do ochrony danych osobowych:

1) znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2016 r. poz. 1654 oraz z 2017 r. poz. 773), ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652), ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2017 r. poz. 1904, 2405 oraz z 2018 r. poz. 5, 106, 138 i 201), ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2017 r. poz. 2226 oraz 2018 r. poz. 201), ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475), ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396 oraz z 2016 r. poz. 2205), ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2017 r.

poz. 1767 oraz z 2018 r. poz. 5) oraz wydanych na ich podstawie aktów wykonawczych;

2) przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego.

Przywołane w pkt 1 ustawy określają z jednej strony zasady sprawowania wymiaru sprawiedliwości, z drugiej zaś strony prawa osób, których dane dotyczą a będących uczestnikami postępowań.

Jako czynnik determinujący przyjęcie wyłączenia przedmiotowego określonego w art. 3 pkt 1 projektu należy wskazać zakres pojęciowy definicji zbioru danych. Definicja zbioru danych, zawarta w art. 3 pkt 6 dyrektywy, jest tożsama z definicją zawartą uprzednio w art. 2 lit c. dyrektywy 95/46/WE oraz art. 7 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych – co oznacza, że do zbioru danych w dalszym ciągu mają zastosowanie koncepcje wypracowane przez doktrynę i orzecznictwo pod rządami poprzedniej dyrektywy. W świetle doktryny i orzecznictwa, zbiór danych, zdefiniowany w art. 3 pkt 6 dyrektywy, powinien zatem spełniać następujące kryteria:

1) musi to być zestaw danych osobowych;
2) dane osobowe w tym zbiorze muszą być uporządkowane w taki sposób, aby można było odszukać żądaną informację bez potrzeby przeszukiwania całego zbioru;
3) dane muszą być uporządkowane według co najmniej dwóch określonych kryteriów, przy czym kryteria te powinny się odnosić do osób fizycznych, a więc zbiór ma być uporządkowany w taki sposób, aby można było odszukać dane osobowe bez potrzeby przeszukiwania całego zbioru.

Oznacza to, że dyrektywy nie stosuje się do akt, takich jak akta postępowania karnego. Akta są wyłączone spod definicji zbioru danych osobowych z trzech powodów:

1) nie są zbiorem danych osobowych.

Dane zawarte w zbiorze muszą być danymi o charakterze osobowym. Tymczasem w aktach spraw i czynności prowadzonych na podstawie ustaw wskazanych w art. 3 pkt 1 gromadzi się różnego rodzaju informacje i materiały dowodowe, na podstawie których organ prowadzący postępowanie i wydający rozstrzygnięcie kształtuje swoje stanowisko co do faktu popełnienia czynu zabronionego, sprawcy tego czynu oraz

odpowiedzialności karnej. Gromadzone i dokumentowane w aktach spraw i czynności dowody nie tworzą zbioru danych. Sam fakt, że dokument, pośród innych informacji, zawiera między innymi dane osobowe nie sprawia, że dokument taki staje się zestawem danych osobowych, a tym bardziej zbiorem danych. Trybunał Sprawiedliwości w wyroku z dnia 17 lipca 2014 r. w połączonych sprawach C 141/12 i C 372/12 wskazał, że dokumenty, w których zawarte są dane osobowe, na przykład dotycząca danej osoby analiza prawna, nie nabierają przez to charakteru „danych osobowych" w rozumieniu prawa unijnego. Nie stanowią zatem danych osobowych, ani tym bardziej zestawu takich danych, dokumenty wchodzące w skład akt, np. protokół przesłuchania czy wyrok z uzasadnieniem. Co za tym idzie, zbiór gromadzący takie dokumenty nie jest zbiorem danych osobowych;

2) nie są uporządkowane w rozumieniu dyrektywy.

Zgodnie z poglądami doktryny prawa (np. W. Zimny), o uporządkowaniu danych osobowych możemy mówić wówczas, gdy dane są przedstawiane w określonym przestrzennym rozmieszczeniu albo w określonej fizycznej czy logicznej strukturze, co w oczywisty sposób nie ma zastosowania do akt postępowania karnego. Z poglądem tym stoi w zgodzie również orzecznictwo, wskazujące, że zestaw danych, podlegający definicji zawartej w prawie unijnym, musi posiadać strukturę, rozumianą jako jednorodna budowa zbioru (np. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 29 kwietnia 2015 r. sygn. II SA/Wa 1604/14). Również motyw 18 preambuły dyrektywy stanowi, że „Zbiory lub zestawy zbiorów, jak i ich strony tytułowe, które nie są uporządkowane według określonych kryteriów, nie powinny wchodzić w zakres stosowania niniejszej dyrektywy.". Zbiór danych nie może być zatem luźnym zestawem, ale musi być zbiorem jednorodnym. Co więcej, powinien posiadać cechy pozwalające na odnalezienie informacji bez potrzeby przeglądania całego zestawu. Takich cech brak w przypadku akt spraw i czynności, gdyż ani nie stanowią one jednorodnego zestawu, ani nie można w nich wyszukać według określonych kryteriów danych osobowych zawartych w materiale dowodowym;

3) kryteria porządkujące akta nie dotyczą danych osobowych.

Zgodnie z definicją zbioru zawartą w art. 3 pkt 6 dyrektywy, dane osobowe w zbiorze muszą być uporządkowane według co najmniej dwóch kryteriów. Należy podkreślić, że wymóg istnienia kryteriów porządkujących dotyczy nie zbioru jako takiego, ale zawartych w nim danych osobowych. Toteż w doktrynie wskazywano (np. Arvid

Mednis), że akta sądowe nie stanowią zbioru danych, gdyż nie są uporządkowane w oparciu o kryteria dotyczące osób fizycznych. Na osobowe kryterium wyszukiwania jako warunek uznania zbioru za zbiór danych osobowych wskazywały również polskie sądy administracyjne (np. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 16 marca 2007 r., II SA/Wa 2110/06483). Tym, co odróżnia zbiór danych osobowych, w rozumieniu prawa unijnego, od innych zestawów danych, jest istnienie cechy lub cech pozwalających na odnalezienie informacji bez potrzeby przeglądania całego zestawu. Toteż nie każdy zestaw informacji zawierający dane osobowe będzie zbiorem danych osobowych w rozumieniu dyrektywy. Będzie nim tylko taki zestaw, w którym dostęp do danych będzie możliwy przez jakiekolwiek kryterium osobowe, np. imię, nazwisko, numer PESEL. Doktryna wskazuje, że uporządkowanie (struktura) zbioru może odnosić się albo do indywidualnych osób (oznaczonych np. nazwiskiem lub numerem identyfikacyjnym), albo do kryteriów grupowych stosowanych do większej liczby osób (np. wiek, wykonywana praca, preferencje co do zakupów, prawo do określonych przywilejów, członkostwo w organizacjach). Akta sprawy karnej nie są zorganizowane według kryteriów dotyczących osób fizycznych. Co więcej, sposób ich prowadzenia w ogóle nie uwzględnia kwestii ułatwienia dostępu do danych osobowych. Kryteria, według których organizowane są akta, odnoszą się nie do danych osobowych, a do kolejności przeprowadzania dowodów lub wątków postępowania dotyczących zwykle odrębnych czynów zabronionych. Kryteria te nie pozwalają na wyszukiwanie danych osobowych, które są rozproszone po całym materiale dowodowym. Akta sprawy również z tego względu nie spełniają definicji zawartej w art. 3 pkt 6 dyrektywy.

Z powyższych trzech względów akta spraw wskazanych w art. 3 pkt 1 nie stanowią zbioru danych, a zatem dyrektywa nie ma do nich zastosowania. Nie oznacza to jednak, że dane osobowe zawarte w aktach są w obecnym stanie prawnym wyłączone spod ochrony prawnej. Postępowanie karne (a także jego odmiany, wskazane w art. 3 pkt 1) nakierowane jest przede wszystkim na to, aby sprawca przestępstwa został wykryty i poniósł karę, zaś osoba niewinna nie poniosła odpowiedzialności karnej. Dane osobowe uzyskane w toku postępowania podlegają zwiększonej ochronie w stosunku do ochrony przewidzianej dyrektywą, gdyż rygory w odniesieniu do ich przetwarzania i ujawniania są surowsze. Podstawą do przetwarzania danych w postępowaniem karnym są przepisy procedury karnej. Przetwarzaniu podlegają dane uzyskane zgodnie

z określonymi wymogami formalnymi, przy czym dane te nie mogą być ujawniane w warunkach innych niż określone w przepisach. W postępowaniu karnym muszą być np. zachowane wymogi i ograniczenia określone w art. 156 k.p.k., zaś ujawnienie danych z tego postępowania, zależnie od stanu faktycznego, może stanowić przestępstwo określone w art. 266 k.k. lub art. 241 k.k., a także uchybienie dyscyplinarne związane z naruszeniem art. 102 *ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze* czy art. 85 *ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych.* Z uwagi na to, dane zawarte w aktach postępowań wskazanych w art. 3 są i pozostaną chronione na podstawie przepisów normujących poszczególne rodzaje procedur wskazanych w przytoczonym przepisie.

Dyrektywa przewiduje możliwość wprowadzenia odmiennego reżimu, odnoszącego się do postępowań karnych. Zgodnie z art. 18 dyrektywy, a także motywami 20 i 49 jej preambuły, ustawodawca krajowy może w taki sposób ukształtować ochronę danych osobowych, zgromadzonych w toku postępowań o charakterze karnym, aby pozostawało to w zgodzie z krajową procedurą, regulującą te postępowania. W motywie 20 dyrektywy prawodawca unijny wskazał też, że dyrektywa nie powinna stanowić dla państw członkowskich przeszkody w określaniu w krajowym prawie karnym procesowym operacji i procedur przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Należy ponadto zauważyć, że Unia Europejska przewiduje liczne gwarancje ochrony prawnej dla obywateli, ale może to czynić jedynie w ramach własnych kompetencji. Najważniejsze zadania państwa, jak zapewnienie bezpieczeństwa wewnętrznego, pozostają nadal domeną kompetencji krajowych. Na prawo do ochrony danych osobowych, trzeba zatem patrzeć przez pryzmat innych praw, mających pierwszeństwo w pewnej hierarchii praw podstawowych. Prawo to doznaje bowiem ograniczeń – przy zachowaniu zasad subsydiarności i proporcjonalności – w sytuacji, gdy może ono naruszyć prawo podstawowe, stojącym wyżej w hierarchii praw. Należy ponadto zauważyć, że obywatele mają prawo oczekiwać od organów państwa, aby postępowania karne przebiegały sprawnie i skutecznie, a bezpieczeństwo świadków i pokrzywdzonych było chronione. Ujawnienie informacji z akt postępowania przygotowawczego może narazić te prawa i zniweczyć cel postępowania. Z tego względu zarówno prawodawca unijny, jak ustawodawca krajowy powinni zachowywać szczególną ostrożność w regulacji uprawnień związanych z realizacją ochrony danych osobowych w postępowaniu

karnym. Podobna ostrożność wynika z brzmienia motywów preambuły dyrektywy, np. motywu 20 i 27, a przede wszystkim motywu 14. Prawodawca unijny w tym ostatnim zapisie wyraźnie podkreślił subsydiarny charakter regulacji związanych z ochroną danych osobowych w stosunku do pierwotnego priorytetu, jakim jest zapewnienie bezpieczeństwa.

Ze stosowania przepisów projektowanej ustawy wyłączono także sferę bezpieczeństwa narodowego, w tym – z perspektywy instytucjonalnej – służby specjalne, to jest Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne. Należy podkreślić, że dyrektywa 2016/680 dopuszcza takie rozwiązanie. W art. 2 ust. 3 lit. a wskazuje, że nie ma ona zastosowania do przetwarzania danych osobowych w ramach działalności nieobjętej obszarem prawa Unii. W tym kontekście należy przypomnieć, że Traktat o Unii Europejskiej w art. 4 ust. 2 (zdanie trzecie) stanowi, że w szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego. Jednocześnie przepis art. 2 ust. 3 lit. a dyrektywy powinien być odczytywany z uwzględnieniem motywu (14), który precyzuje zakres stosowania dyrektywy. Zgodnie z brzmieniem motywu (14) przepisy dyrektywy nie powinny mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii. Jednocześnie pojęcie działalności wykraczającej poza zakres prawa Unii jest rozwijane przez wskazanie trzech obszarów, które obejmuje: (1) czynności w zakresie bezpieczeństwa narodowego, (2) czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym oraz (3) przetwarzanie danych osobowych przez państwa członkowskie podczas czynności, które wchodzą w zakres zastosowania tytułu V rozdział 2 Traktatu o Unii Europejskiej. Należy zauważyć, że prawodawca europejski odrębnie wymienia czynności w zakresie bezpieczeństwa narodowego oraz czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym. Oznacza to, że poza zakresem dyrektywy znajdują się zarówno poszczególne czynności z zakresu bezpieczeństwa narodowego (wykonywane przez dowolne podmioty, którym przepisy powierzają takie zadania), jak wszystkie czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym. W tym drugim przypadku wyłączenie ma charakter *de facto* podmiotowy, gdyż dotyczy wszystkich czynności podmiotów, które zajmują się bezpieczeństwem narodowym. W tym kontekście należy zauważyć, że w polskim porządku prawnym podmiotami

zajmującymi się bezpieczeństwem narodowym są służby specjalne, w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W szczególności należy przywołać ustawę o ABW oraz AW, która wskazuje, że ABW jest właściwa w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego (art. 1), a AW w sprawach ochrony bezpieczeństwa zewnętrznego państwa (art. 2). Zgodnie z ustawą z dnia 9 czerwca 2016 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego SKW jest właściwa w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej (art. 1), a SWW w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej SZ RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej (art. 2). Z kolei zgodnie z ustawą z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym do zadań CBA należy w szczególności zwalczanie działalności godzącej w interesy ekonomiczne państwa (art. 1 ust. 1). Należy podkreślić, że wszystkie przywołane tu obszary działalności mieszczą się w zakresie pojęcia bezpieczeństwa narodowego, stanowiąc jego składowe. Dlatego też wszystkie wymienione służby specjalne są agencjami lub jednostkami zajmującymi bezpieczeństwem narodowym w rozumieniu motywu (14) dyrektywy. Z tego też względu spełnione zostają przesłanki ich wyłączenia z zakresu obwiązywania tego aktu. Dyrektywa 2016/680 nie ma zastosowania do czynności podmiotów zajmujących się bezpieczeństwem narodowym (art. 2 ust. 3 lit. a w zw. z motywem 14 dyrektywy), a zatem, w polskim systemie prawnym nie powinna być stosowana, do służb specjalnych, tj. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego. Realizacja szczegółowo określonych, ustawowych zadań każdego z wymienionych podmiotów ma na celu zapewnienie bezpieczeństwa narodowego, w różnych jego aspektach – zgodnie z zakresem kompetencyjnym każdej ze służb – co przemawia za podmiotowym wyłączeniem z zakresu regulacji projektowanej ustawy.

W części projektu zawierającej wyjaśnienie terminologii stosowanej w ustawie (art. 4) posłużono się w znacznej mierze definicjami zawartymi w art. 3 dyrektywy 2016/680.

W tym kontekście szczególną uwagę należy zwrócić na definicję pojęcia „danych osobowych”, za które uważa się dane osobowe, o których mowa w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1). Rozwiązanie to zachowuje zatem pełną zgodność z przepisami dyrektywy 2016/680.

Natomiast pod pojęciem „przetwarzania” rozumie się operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Rozdział 2 projektu poświęcony został zadaniom organu nadzorczego. Funkcję organu nadzorczego w ramach dyrektywy 2016/680 pełnił będzie Prezes Urzędu Ochrony Danych Osobowych (dalej zwany „Prezesem Urzędu”) powołany na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Skorzystano w tym przypadku z przewidzianej w art. 41 ust. 3 dyrektywy 2016/680 możliwości, aby organem tym był organ nadzorczy ustanowiony na mocy rozporządzenia 2016/679. Rozwiązanie to jest korzystne nie tylko ze względów ekonomicznych (nie ma potrzeby tworzenia odrębnego urzędu), ale przede wszystkim gwarantuje spójność systemu ochrony danych osobowych, a przez to ich większe bezpieczeństwo. W ten sposób zapewniono również niezależność organu nadzorczego stanowiącą nieodzowny element całego systemu.

Z uwagi na podobny sposób określenia niektórych zadań organu nadzorczego w rozporządzeniu 2016/679 oraz dyrektywie 2016/680, a także ze względu na to, że ustanowiony będzie jeden wspólny organ nadzorczy dla tych dwóch reżimów prawnych, w projektowanym art. 6 skupiono się na zadaniach Prezesa Urzędu, wynikających ze specyfiki przetwarzania danych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar

porządkowych i środków przymusu skutkujących pozbawieniem wolności. Mając na uwadze powyższe, wśród zadań Prezesa Urzędu wskazano:

1) monitorowanie i egzekwowanie stosowania przepisów niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych;
2) upowszechnianie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych, w celu o którym mowa w art. 1 pkt 1 oraz rozumieniem tych zjawisk;
3) doradzanie instytucjom publicznym w sprawach środków ochrony praw i wolności osób fizycznych z związku z przetwarzaniem danych osobowych, w celu o którym mowa w art. 1 pkt 1;
4) upowszechnianie wiedzy z zakresu stosowania niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych wśród administratorów i podmiotów przetwarzających;
5) udzielanie osobie, której dane dotyczą, na jej żądanie, informacji o wykonywaniu praw przysługujących jej na mocy niniejszej ustawy, a w miarę potrzeby współpracowanie w tym celu z organami nadzorczymi w innych państwach Unii Europejskiej;
6) rozpatrywanie skarg osób, których dane osobowe są przetwarzane niezgodnie z prawem i prowadzenie postępowań w tym zakresie;
7) o ile przepis szczególny nie stanowi inaczej, kontrola zgodności przetwarzania danych osobowych z przepisami niniejszej ustawy;
8) prowadzenie postępowania w sprawie stosowania niniejszej ustawy, w tym na podstawie informacji otrzymanych od innego organu publicznego;
9) pełnienie funkcji konsultacyjnych, o których mowa w art. 38, dotyczących operacji przetwarzania w ramach niniejszej ustawy;
10) współpraca z organami nadzorczymi w państwach członkowskich Unii Europejskiej;
11) wydawanie opinii dla Sejmu, Senatu oraz innych organów władzy publicznej w sprawach ochrony danych osobowych;
12) wydawanie opinii w odniesieniu do projektów aktów prawnych w sprawach dotyczących ochrony danych osobowych,

Prezes Urzędu dysponował będzie również możliwością przeprowadzania kontroli przetwarzania danych osobowych, wykorzystując w tym celu procedury uregulowane

w rozdziale 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, poza przepisami nieadekwatnymi do specyfiki przetwarzania danych osobowych w zakresie wynikającym z dyrektywy 2016/680. Rozwiązanie to stanowi dodatkowy element gwarancyjny w maksymalny sposób zbliżający oba systemy ochrony danych osobowych, ale uwzględniające jednocześnie ich specyfikę.

Kierując się wspomnianą specyfiką, określono również uprawnienia kontrolującego (art. 7 projektu), który w toku kontroli ma prawo wglądu do zbioru danych zawierającego dane osobowe oraz do innych dokumentów mających bezpośredni związek z przedmiotem kontroli jedynie w obecności upoważnionego przedstawiciela właściwego organu, w którym jest przeprowadzana kontrola. Zapewnienie kontrolującemu wglądu do zbioru danych oraz do innych dokumentów mających bezpośredni związek z kontrolą odbywać się będzie z zachowaniem przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Zgodnie z projektowanymi przepisami (art. 8 ust. 1) w przypadku uzasadnionego podejrzenia, że planowane operacje przetwarzania mogą skutkować naruszeniem projektowanych przepisów, Prezes Urzędu wydaje administratorowi lub podmiotowi przetwarzającemu ostrzeżenie.

Z kolei w przypadku naruszenia przepisów o ochronie danych osobowych, Prezes Urzędu w drodze decyzji administracyjnej, nakazuje administratorowi lub podmiotowi przetwarzającemu przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień;
2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;
3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;
4) zabezpieczenie danych lub przekazanie ich innym podmiotom;
5) usunięcie danych osobowych;
6) wprowadzenie czasowych lub stałych ograniczeń przetwarzania i przekazywania, w tym zakazu przetwarzania.

Jednocześnie powyższa decyzja Prezesa Urzędu nie może nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Administrator w przypadku uznania, że zgromadzone w ten sposób dane są zbędne, jest zobowiązany do ich usunięcia. W przypadku

niedopełnienia obowiązku usunięcia danych osobowych przez administratora Prezes Urzędu może nakazać ich usunięcie. W celu realizacji uprawnienia Prezes Urzędu nie uzyskuje dostępu do danych osobowych zgromadzonych w toku tych czynności (art. 8 ust. 3). Z uwagi na specyficzny, a także niejawny charakter tego rodzaju czynności, przepis ten umożliwia dalsze przetwarzanie danych uzyskanych z naruszeniem przepisów projektowanej ustawy. Rozwiązanie to nie wyłącza jednak możliwości skorzystania przez organ nadzorczy z pozostałych mechanizmów gwarancyjnych. Ponadto administrator lub podmiot przetwarzający będzie zobowiązany, bez zbędnej zwłoki, do przywrócenia zgodnego z prawem sposobu przetwarzania danych osobowych.

W projektowanym art. 11 przewidziano dodatkowo możliwość wystąpienia przez Prezesa Urzędu bezpośrednio do inspektora danych osobowych – o którym szerzej napisano w dalszej części uzasadnienia – o przeprowadzenie sprawdzenia stosowania przepisów projektowanej ustawy przez administratora, który tego inspektora powołał. Jednocześnie przeprowadzenie tego rodzaju sprawdzenia, nie wyłącza prawa Prezesa Urzędu do przeprowadzenia przez niego kontroli (art. 11 ust. 3).

W art. 12 projektu przyjęto rozwiązanie, zgodnie z którym w sprawach objętych zakresem regulacji rozdziału 2 do prowadzonych postępowań stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257), o ile przepisy projektowanej ustawy nie stanowią inaczej. Decyzje Prezesa Urzędu podlegają z kolei zaskarżeniu do sądu administracyjnego.

W rozdziale 3 projektowanej ustawy znalazły się uregulowania dotyczące zasad przetwarzania danych osobowych. Oprócz ogólnych przepisów odnoszących się do konieczności przestrzegania przepisów prawa (art. 13 ust. 1) oraz zgodności z celami przetwarzania danych, określonymi w ustawie (art. 13 ust. 2), w projektowanych przepisach przewidziano również sytuację, gdy dane zebrane pierwotnie w jednym z celów przewidzianych przez ustawę będą przetwarzane w innym, ale również przewidzianym przez projektowaną ustawę, celu (art. 13 ust. 3).

Ustawa dopuszcza również dalsze przetwarzanie danych do innych, nieprzewidzianych przez projektowane przepisy celów w zakresie niezbędnym do ich archiwizacji w interesie publicznym oraz do celów: naukowych, statystycznych lub historycznych, o ile podlega ono odpowiednim zabezpieczeniom praw i wolności osób, których dane

dotyczą (art. 13 ust. 4). W tym przypadku zastosowanie będą miały przepisy rozporządzenia 2016/679.

Projektowana ustawa, co do zasady, zabrania przetwarzania danych osobowych, określanych jako wrażliwe, które z racji swojego charakteru mają szczególne znaczenie w świetle podstawowych praw i wolności, wymagając szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko naruszenia podstawowych praw i wolności. Chodzi przede wszystkim o dane osobowe ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej (art. 14 ust. 1).

Mając jednakże na uwadze wytyczne sformułowane w motywach (37) i (51) oraz w art. 10 dyrektywy 2016/680, przetwarzanie tego rodzaju danych dopuszczono jeżeli: przepisy prawa, w tym prawa Unii Europejskiej zezwalają na ich przetwarzanie, jest to niezbędne dla ochrony życia lub zdrowia osoby, której dane dotyczą lub innej osoby lub dane takie zostały upublicznione przez osobę, której dotyczą (art. 14 ust. 2). W projektowanych przepisach zagwarantowano, aby ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, mające dla niej niekorzystne skutki prawne lub poważnie na nią wpływające, nie były podejmowane wyłącznie w wyniku przetwarzania danych osobowych w sposób zautomatyzowany, w tym w wyniku profilowania, chyba że dopuszcza je prawo Unii Europejskiej lub odrębne przepisy, którym podlega administrator i które przewidują odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą. Minimum wymaganym w takich przypadkach to możliwość uzyskania interwencji ze strony administratora (art. 15 ust. 1). Projektowana ustawa zabrania również, aby rozstrzygnięcia takie podejmowane były na podstawie danych wrażliwych (art. 15 ust. 2), które nie mogą być również wykorzystywane do profilowania osób fizycznych (art. 15 ust. 3).

W art. 16 projektu ustawy wprowadzono obowiązek weryfikacji przez administratorów danych osobowych w terminach określonych przez przepisy szczególne, regulujące działania właściwego organu, a jeżeli przepisy te nie określają terminu – nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych. Weryfikacja będzie dokonywana w celu ustalenia, czy istnieją dane, których dalsze przechowywanie

jest zbędne. Zbędne dane będą usuwane. Wprowadzenie powyższego przepisu stanowi realizację dyspozycji art. 5 dyrektywy 2016/680 obligującego do przyjęcia odpowiednich terminów usuwania danych osobowych lub okresowego przeglądu konieczności ich przechowywania. Jednocześnie w projekcie ustawy przewidziano, że dane osobowe uznane za zbędne można przekształcić w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, iż przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań (art. 17).

Kierując się treścią motywu (31) dyrektywy 2016/680, zgodnie z którym w stosownych przypadkach należy w jak największym stopniu wyraźnie rozróżniać dane osobowe różnych kategorii osób, których dane dotyczą, a także w oparciu o sposób sformułowania art. 6 dyrektywy 2016/680, zaproponowano w art. 19 projektu, aby o ile rozróżnienie to jest możliwe lub nie jest dalece utrudnione, administrator zapewniał podział na dane osobowe dotyczące:

1) osób, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
2) osób skazanych za czyn zabroniony;
3) pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;
4) innych osób związanych z czynem zabronionym, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania, osób, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w pkt 1 i 2.

Sposób sformułowania powyższego oraz określone w nim kryteria stanowią bezpośrednie odzwierciedlenie przywołanych przepisów dyrektywy 2016/680.

Art. 7 dyrektywy 2016/680 zobowiązuje państwa członkowskie do zapewnienia, by dane osobowe oparte na faktach były rozróżniane, tak dalece, jak to możliwe, z danymi osobowymi opartymi na indywidualnych ocenach. W projekcie ustawy transpozycja tego przepisu dokonana została w art. 20, z wyłączeniem przypadków gdy dokonanie takiego rozróżnienia nie jest możliwe lub dalece utrudnione.

Kolejny przepis w tej części projektowanej ustawy (art. 21) umożliwia przesyłanie lub udostępnianie danych osobowych innym właściwym organom, państwu trzeciemu lub organizacji międzynarodowej. Działania takie możliwe są po uprzednim zweryfikowaniu, w miarę potrzeby i możliwości, prawidłowości, kompletności i aktualności tych danych. Jednocześnie wraz z danymi przesyłane są informacje pozwalające odbiorcy ocenić stopień prawidłowości i kompletności tych danych oraz stopień ich aktualności. Z kolei w przypadku przesłania danych nieprawdziwych, niekompletnych lub nieaktualnych lub przesłania danych osobowych z naruszeniem przepisów projektowanej ustawy, właściwy organ, który takie dane przesłał, jest obowiązany, bez zbędnej zwłoki, poinformować o tym odbiorcę oraz sprostować, uzupełnić lub uaktualnić te dane, a także przesłać odbiorcy dane właściwe, chyba że z uwagi na upływ czasu jest to oczywiście nieuzasadnione, albo usunąć lub ograniczyć ich przetwarzanie, a także poinformować o tym odbiorcę w celu usunięcia lub ograniczenia ich przetwarzania.

W rozdziale 4 projektu ustawy, znalazły się regulacje w zakresie praw osoby, której dane dotyczą. W art. 24 określony został obowiązek informacyjny realizowany przez administratora, przy czym ust. 1 i 3 stanowią implementację obowiązku informacyjnego wynikającego z art. 13 ust. 1–2 dyrektywy, zaś ust. 4 – obowiązku informacyjnego określonego w art. 14 dyrektywy. Mając na względzie, że przepisy dyrektywy odmiennie określają charakter tego obowiązku w każdym z cytowanych artykułów, w projekcie określono, że obowiązek wynikający z ust. 1 i 3 realizowany jest przez administratora z urzędu, zaś określony w ust. 4 – na wniosek osoby, której dane dotyczą. W projekcie określono również prawo osoby, której dane dotyczą do dostępu do jej danych osobowych (art. 23 ust. 1), przy czym prawo to zostało określone, jako udostępnienie lub przekazanie wnioskodawcy kopii danych osobowych albo sporządzonego w przystępnej formie wyciągu z tych danych (ust. 2). Tak zdefiniowane prawo dostępu jest zgodne z wyjaśnieniem zawartym w motywie (43) preambuły dyrektywy. Zgodnie z art. 24 ust. 1 osoba, której dane dotyczą może wystąpić do administratora z wnioskiem o:

1) uzupełnienie, uaktualnienie lub sprostowanie danych osobowych – w przypadku gdy dane te są niekompletne, nieaktualne lub nieprawdziwe;
2) usunięcie danych osobowych – w przypadku gdy dane te zostały zebrane lub są przetwarzane z naruszeniem przepisów niniejszej ustawy.

W przypadku stwierdzenia, że dane są niekompletne, nieaktualne lub nieprawdziwe administrator dokonuje ich usunięcia z urzędu. Jeżeli wniosek o sprostowanie lub uaktualnienie dotyczy danych, które znajdują się również w dokumencie zawierającym zeznanie, wypowiedź czy oświadczenie osoby fizycznej, a ustalono, że dane te są nieprawdziwe lub nieaktualne, administrator pozostawia je w postaci niezmienionej. Wniosek taki uwzględnia się tylko przez umieszczenie w zbiorze danych stosownej adnotacji (art. 24 ust. 3). Reguła określona w ust. 3 jest zgodna z wyjaśnieniem zawartym w motywie (30 i 47) preambuły dyrektywy.

Zgodnie z projektowanym art. 25 ustawy administrator jest obowiązany, bez zbędnej zwłoki, do czasowego ograniczenia przetwarzania danych osobowych jeżeli:

1) osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić;
2) dane osobowe, które podlegają usunięciu, muszą zostać zachowane do celów dowodowych.

Czasowe ograniczanie przetwarzania danych osobowych polega na nieudostępnianiu tych danych odbiorcom. Administrator jest również zobowiązany do poinformowania organu, od którego nieprawdziwe dane osobowe pochodzą o sprostowaniu danych. Informuje również odbiorców o dokonanym sprostowaniu lub usunięciu danych osobowych lub ograniczeniu ich przetwarzania. W takiej sytuacji odbiorcy również mają obowiązek uaktualnić, sprostować, usunąć dane osobowe lub ograniczyć ich przetwarzanie.

W art. 26 ust. 1 określono przesłanki, których zaistnienie warunkuje nieprzekazanie informacji określonych w przepisach rozdziału 4 lub odmowę dostępu do danych osobowych, jeżeli mogłoby to spowodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia i wykroczenia skarbowe;
4) zagrożenie dla życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;
5) zagrożenie dla bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa:

6) istotne naruszenie dóbr osobistych innych osób.

W przypadku, o którym mowa w art. 26 ust. 1, administrator poucza osobę, której dane dotyczą, o możliwości wniesienia skargi do Prezesa Urzędu. W odniesieniu do danych osobowych zgromadzonych w postępowaniach, o których mowa w art. 3 pkt 1, prawa osób, których dane dotyczą, są wykonywane wyłącznie na podstawie i w zakresie przewidzianym przez przepisy regulujące te postępowania (art. 27). Wprowadzenie możliwości nieudzielania informacji przez administratora oparte zostało na sformułowanych w dyrektywie 2016/680 przesłankach, określonych w art. 13 ust. 3 oraz art. 15 ust. 1 i 3 zdanie drugie. Szersze wyjaśnienie tej kwestii znajdujące się w motywie (44) dyrektywy 2016/680, który wskazuje że rozwiązanie to ma uniemożliwić zakłócanie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub czynności procesowych, uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, oraz w celu ochrony bezpieczeństwa publicznego lub narodowego, a także aby chronić prawa i wolności innych osób.

Z wyjątkiem wymienionych wyżej sytuacji nieudzielenia informacji, administrator pisemnie informuje osobę, której dane dotyczą, o każdej odmowie uaktualnienia, sprostowania lub usunięcia danych osobowych, lub ograniczenia ich przetwarzania, oraz o przyczynach tej odmowy.

W celu ograniczenia składania wniosków przez osoby nieuprawnione wskazano, że wnioskodawca jest zobowiązany do podania co najmniej imienia i nazwiska oraz adresu korespondencyjnego. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby, która złożyła wniosek, może on zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości tej osoby.

Zgodnie z art. 12 dyrektywy 2016/680 w projektowanych przepisach określono, że administrator podejmuje działania mające na celu ułatwienie osobie, której dane dotyczą przysługujących jej praw (art. 30 ust. 1), wskazując jednocześnie, że udziela tej osobie informacji jasnym i prostym językiem, co do zasady w takiej postaci, w jakiej wniesiono wniosek, chyba że powodowałoby to nadmierne trudności lub koszty, lub przepis ustawy zastrzega inną formę udzielenia wnioskodawcy odpowiedzi (art. 30 ust. 2). Jako zasadę wprowadzono niepobieranie opłat za czynności podejmowane przez administratora na wniosek osoby, której dane dotyczą. Również wnioski osób, które

realizowane będą w sposób określony w art. 27 projektu, będą wolne od opłat. Wprawdzie reguła ta nie jest wyrażona bezpośrednio w przepisach proceduralnych reagujących postępowanie karne, ale wynika z braku przepisu określającego takie opłaty. Jeżeli jednak żądania takie są w sposób oczywisty nieuzasadnione lub nadmierne, zwłaszcza ze względu na ich powtarzalność, administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań lub odmówić podjęcia działań w związku z żądaniem (art. 30 ust. 4). W tej sytuacji administrator, bez zbędnej zwłoki, lecz nie później niż w terminie 14 dni od dnia złożenia wniosku powiadomi wnioskodawcę o wysokości opłaty, o której mowa w ust. 4 pkt 1. Udzielenie informacji zgodnie z wnioskiem następuje po upływie 14 dni od dnia powiadomienia wnioskodawcy, chyba że wnioskodawca dokona w tym terminie zmiany wniosku co do zakresu żądanych danych, sposobu lub formy ich udostępnienia albo wycofa wniosek. Przepis ten, zgodnie z intencją ustawodawcy europejskiego wyrażoną również w motywie (40) dyrektywy 2016/680, ma zapobiegać wykorzystywania powyższych uprawnień w celu sparaliżowania pracy administratora.

Rozdział kolejny (5) dotyczy administratora i podmiotu przetwarzającego. Administrator odpowiedzialny jest przede wszystkim za zapewnienie, aby dane osobowe były (art. 31 ust. 1):

1) przetwarzane zgodnie z prawem i rzetelnie oraz przy zastosowaniu niezbędnych środków technicznych i organizacyjnych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
2) przetwarzane w konkretnych i uzasadnionych celach;
3) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;
5) przechowywane w formie umożliwiającej identyfikacje osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;
6) 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 środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczone przed ich

udostępnieniem osobom nieupoważnionym lub wejście w posiadanie przez osobę nieuprawnioną.

Jednocześnie, mając na uwadze treść art. 19 ust. 2 dyrektywy 2016/680, w projekcie (art. 31 ust. 4) zobowiązano administratora do opracowania i wdrożenia polityki ochrony danych, uwzględniając w niej sposób dokumentowania środków technicznych i organizacyjnych stosowanych do zapewnienia ochrony danych osobowych, do których należą (art. 39):

1) uniemożliwienie osobom nieuprawnionym dostępu do sprzętu używanego do przetwarzania (kontrola dostępu do sprzętu);
2) zapobiegnięcie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
3) zapobiegnięcie nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);
4) zapobiegnięcie korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);
5) zapewnienie osobom, uprawnionym do korzystania z systemu zautomatyzowanego przetwarzania, dostępu wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);
6) umożliwienie zweryfikowania i ustalenia podmiotów, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione, za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);
7) umożliwienie następczej weryfikacji i ustalenia, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (kontrola wprowadzania danych);
8) zapobieżenie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);
9) zapewnienie przywrócenia zainstalowanych systemów w razie awarii (odzyskiwanie);

10) zapewnienie działania funkcji systemu, zgłaszania występujących w nich błędów (niezawodność) oraz odporności przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

Jednym z nowych rozwiązań przewidzianych przez dyrektywę 2016/680, które zostało wprowadzone w projekcie niniejszej ustawy, jest zobowiązanie administratora, aby już w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, planował zastosowanie odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja, a jednocześnie chronił prawa osób, których dane dotyczą (art. 32). Jeżeli kilku administratorów wspólnie ustali cel i sposoby przetwarzania danych osobowych stają się oni współadministratorami (art. 33), a ustawa określa mechanizmy podziału zadań między nimi.

Administrator może również w drodze pisemnej umowy (dopuszczalna jest również postać elektroniczna) powierzyć przetwarzanie danych innemu podmiotowi, czyli tzw. podmiotowi przetwarzającemu (art. 34 ust. 1). Rozwiązanie to zawiera instrumenty gwarancyjne niepozwalające na obniżenie standardu ochrony danych w tego rodzaju sytuacjach. Umowa określa w szczególności (art. 34 ust. 3):

1) przedmiot i okres jej obowiązywania;
2) charakter i cel przetwarzania;
3) rodzaj przetwarzanych danych osobowych;
4) kategorie osób, których dane dotyczą;
5) prawa i obowiązki administratora;
6) obowiązki podmiotu przetwarzającego;
7) sposób prowadzenia przez administratora kontroli przetwarzania danych.

Zawarte w projektowanym art. 34 ust. 5 obowiązki podmiotu przetwarzającego wobec administratora stanowią z jednej strony gwarancję, że będzie on wykonywał swoje zadania zgodnie z przepisami projektowanej ustawy, z drugiej zaś zapewniają administratorowi kontrolę nad działaniami tego podmiotu, między innymi przez zobowiązanie udostępniania administratorowi wszelkich informacji związanych z weryfikacją prawidłowości realizacji umowy powierzenia. Generalnie bowiem odpowiedzialność za przestrzeganie przepisów projektowanej ustawy spoczywa na administratorze, co nie wyłącza odpowiedzialności podmiotu przetwarzającego za przetwarzanie danych niezgodnie z niniejszą ustawą lub umową powierzenia (art. 34 ust. 7–8).

W celu zapewnienia rozliczalności w zakresie przetwarzania danych osobowych administrator oraz podmiot przetwarzający (w powierzonym zakresie) prowadzą, na podstawie projektowanego art. 35, wykaz kategorii czynności przetwarzania obejmujące dane:

1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora, współadministratora, inspektora ochrony oraz podmiotu przetwarzającego;
2) cele przetwarzania;
3) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
4) opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych;
5) informacje o stosowaniu profilowania – w przypadku gdy zostało ono zastosowane;
6) kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
7) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;
8) planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe;
9) ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych, o których mowa w art. 39, jeżeli jest to możliwe.

Dyrektywa 2016/680 w motywie (57) oraz w art. 25 ust. 1 wprowadziła obowiązek ewidencjonowania operacji przeprowadzanych w zautomatyzowanych systemach przetwarzania, takich jak zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie lub usuwanie danych. Obowiązek ten został wprowadzony w art. 36 projektowanych przepisów, w którym określono również zgodne z dyrektywą 2016/680 cele prowadzenia powyższej ewidencji, a także obowiązek jej udostępniania organowi nadzorczemu.

Nowością wynikającą z dyrektywy 2016/680 jest również obowiązek dokonania wcześniejszej oceny skutków planowanych operacji przetwarzania przez administratora, jeżeli jakiś rodzaj przetwarzania może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych (art. 37), a także wprowadzenie uprzednich

konsultacji z organem nadzorczym, które mają zagwarantować, że utworzenie nowych zbiorów danych będzie zgodne z przepisami projektowanej ustawy oraz przy wykorzystaniu odpowiednich zabezpieczeń, a także odpowiednio wczesną interwencję organu nadzorczego.

W celu zapewnienia odpowiedniego bezpieczeństwa przetwarzanych danych osobowych, administrator lub podmiot przetwarzający mają obowiązek stosować środki techniczne i organizacyjne zapewniające odpowiednią ochronę tych operacji (art. 39). Do przetwarzania danych osobowych może być dopuszczona wyłącznie osoba zapewniająca bezpieczeństwo przetwarzanych danych osobowych oraz posiadająca upoważnienie nadane przez administratora lub podmiot przetwarzający (art. 41). Natomiast administrator musi posiadać ewidencję wszystkich osób, którym takie upoważnienie zostało wydane (art. 42).

W przypadkach gdy nastąpi naruszenie ochrony danych osobowych, administrator bez zbędnej zwłoki, nie później niż w ciągu 72 godzin, musi zgłosić takie naruszenie do Prezesa Urzędu, a w przypadku niedotrzymania tego terminu – zgłosić naruszenie oraz przekazać uzasadnienie przyczyn tej sytuacji. Podobny obowiązek nałożony został na podmiot przetwarzający, który naruszenia takie zgłasza bez zbędnej zwłoki, nie później jednak niż w ciągu 48 godzin, administratorowi.

W przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 45 ust. 1). Zawiadomienie to powinno być sformułowane prostym i jasnym językiem. Wskazane zawiadomienie, nie jest wymagane, jeżeli został spełniony jeden z poniższych warunków (art. 45 ust. 2):

1) administrator zastosował odpowiednie techniczne i organizacyjne środki ochrony, w szczególności szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku (w takim przypadku wydany zostaje publiczny komunikat lub stosuje się podobnym środek).

W ramach realizacji wytycznych dyrektywy 2016/680, projekt ustawy przewiduje także dla administratora obowiązek wyznaczenia inspektora ochrony danych, do którego zadań należy:

1) informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;
2) prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania;
3) monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;
4) monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem;
5) współpraca z Prezesem Urzędu;
6) monitorowanie realizacji zaleceń, o których mowa w art. 38 ust. 4, oraz przedstawianie Prezesowi Urzędu stanu ich realizacji;
7) pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 38, oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach;
8) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37 oraz monitorowanie wykonania ty zaleceń;
9) sporządzanie i przekazywanie administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

Zgodnie z wyjaśnieniem zawartym w motywie (63) dyrektywy 2016/680 inspektor ochrony danych pomaga administratorowi w monitorowaniu wewnętrznego przestrzegania przepisów przyjętych na podstawie dyrektywy. Osoba ta może być członkiem dotychczasowego personelu administratora. Projektowane przepisy dopuszczają również, że kilku administratorów może, uwzględniając swoją strukturę organizacyjną i wielkość, wspólnie wyznaczyć jednego inspektora ochrony danych, na przykład w przypadku dzielonych zasobów w jednostkach centralnych. Osoba ta może

być również mianowana na różne stanowiska w ramach struktury poszczególnych administratorów. Inspektor ochrony danych pomaga również pracownikom przetwarzającym dane osobowe, dostarczając im informacji i porad na temat przestrzegania spoczywających na nich obowiązków w zakresie ochrony danych.

Mając na uwadze szczególną rolę, jaką będzie pełnił inspektor w systemie ochrony danych osobowych, funkcję tę pełnić może osoba, która:

1) ukończyła studia wyższe (wymóg ten jest dodatkowy względem tych wynikających w odniesieniu do inspektorów z rozporządzenia 2016/679 i wynika ze specyfiki zbiorów danych, których dotyczy ustawa i wrażliwości gromadzonych w nich danych);
2) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
3) posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;
4) nie była skazana prawomocnym wyrokiem, orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.

Rozliczenie działalności inspektora następuje na podstawie składanego raz w roku sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

W rozdziale 6 projektowanej ustawy znalazły się uregulowania odnoszące się do współpracy między organami nadzorczymi państw członkowskich. Organy te mogą współpracować w zakresie wymiany informacji, a także prowadzenia konsultacji, kontroli i postępowań.

Środki ochrony prawnej oraz odpowiedzialność prawna stanowią przedmiot rozdziału 7. Podstawowym prawem osoby, której dane osobowe są przetwarzane niezgodnie z prawem, jest prawo wniesienia skargi do Prezesa Urzędu w terminie 30 dni od powzięcia wiadomości o tym naruszeniu lub otrzymania informacji od administratora (art. 50). Prawo do zgłoszenia naruszenia przetwarzania danych osobowych przysługuje również innym osobom w przypadku powzięcia przez nie wiarygodnej wiadomości o tym naruszeniu. Do rozpatrywania zgłoszeń tych osób stosuje się odpowiednio art. 225, art. 231 oraz art. 237–239 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Prezes Urzędu, na uzasadniony wniosek

zgłaszającego, zapewnia poufność jego danych. Ponadto każdemu podmiotowi, wobec którego Prezes Urzędu wydał decyzję przysługuje prawo do wniesienia skargi do sądu administracyjnego na decyzję Prezesa Urzędu (art. 51).

Zgodnie z projektowanym art. 52, osoba, której dane dotyczą, może umocować organizację społeczną o charakterze niezarobkowym, prowadzącą działalność statutową w interesie publicznym i działającą w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych, do wykonywania w jej imieniu praw, w tym wnoszenia przewidzianych przez projektowaną ustawę środków zaskarżenia.

Osobie, która poniosła szkodę lub krzywdę w wyniku czynności naruszających przepisy niniejszej ustawy, na podstawie art. 53 projektu ustawy, przysługuje odszkodowanie lub zadośćuczynienie.

W rozdziale 8 zaproponowano przepisy karne, zgodnie z którymi 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. Jeżeli czyn ten dotyczy danych wrażliwych, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Natomiast kto udaremnia lub istotnie utrudnia kontrolującemu przeprowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat dwóch.

Powyższe przepisy karne są dostosowane do przepisów karnych ustawy wdrażającej do polskiego porządku prawnego rozporządzenie 2016/679.

Przepisy karne zawarte w projektowanej ustawie stanowią jedynie jeden z możliwych, na gruncie polskiego systemu prawa, rodzajów odpowiedzialności za naruszenie przepisów związanych z ochroną danych osobowych. Nie należy zapominać, że zgodnie z art. 231 Kodeksu karnego, każdy funkcjonariusz publiczny może zostać pociągnięty do odpowiedzialności karnej w związku z przekroczeniem uprawnień lub niedopełnieniem obowiązków. Istotne znaczenie ma również kwestia odpowiedzialności dyscyplinarnej za popełnione przewinienie. Jest to tym bardziej istotne, że postępowanie dyscyplinarne jest postępowaniem samoistnym, niezależnym od wyników postępowania karnego.

Transpozycja do polskiego prawa dyrektywy 2016/680 wymaga również dokonania odpowiednich zmian w przepisach ustrojowych właściwych organów w sferze zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, a także zmian w innych przepisach odnoszących się do udostępniania danych tym organom. Przepisy normujące niniejsze zagadnienie znalazły się w rozdziale 9 ustawy. W tym zakresie niezbędne jest dokonanie zmian w następujących przepisach:

1) ustawy z dnia 26 marca 1982 r. o Trybunale Stanu;
2) ustawy z dnia 18 kwietnia 1985 r. o rybactwie śródlądowym;
3) ustawy z dnia 6 kwietnia 1990 r. o Policji;
4) ustawy z dnia 12 października 1990 r. o Straży Granicznej;
5) ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej;
6) ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska;
7) ustawy z dnia 28 września 1991 r. o lasach;
8) ustawy z dnia 13 października 1995 r. – Prawo łowieckie; ustawy z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych;
9) ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne;
10) ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy;
11) ustawy z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych;
12) ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych;
13) ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej;
14) ustawy z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych;
15) ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów wojskowych;
16) ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych;
17) ustawy z dnia 6 września 2001 r. o transporcie drogowym;
18) ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
19) ustawy z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych;
20) ustawy z dnia 28 marca 2003 r. o transporcie kolejowym;

21) ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych;
22) ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
23) ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym;
24) ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;
25) ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych;
26) ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej;
27) ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych;
28) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
29) ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej;
30) ustawy z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym;
31) ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze;
32) ustawy z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych;
33) ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej;
34) ustawy z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym;
35) ustawy z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami;
36) ustawy z dnia 20 lipca 2017 r. – Prawo wodne;
37) ustawy z dnia 8 grudnia 2017 r. o Sądzie Najwyższym;
38) ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa;
39) ustawy z dnia 10 stycznia 2018 r. o szczególnych rozwiązaniach związanych z organizacją w Rzeczypospolitej Polskiej sesji Konferencji Stron Ramowej konwencji Narodów Zjednoczonych w sprawie zmian klimatu;
40) ustawy z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej;
41) ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu;

42) ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera.

Z wyjątkiem przepisów obejmujących zmiany w ustawie z dnia 6 kwietnia 1990 r. o Policji (w zakresie jednoznacznego wskazania właściwości Policji w odniesieniu do przestępstw skarbowych, celem uniknięcia wątpliwości interpretacyjnych, realizacji postulatów *de lege ferenda* w kontekście przeniesienia części przepisów z aktów wykonawczych dotyczących przetwarzania danych i funkcjonujących w Policji systemów bazodanowych na poziom ustawy), a także w ustawie *o szczególnych rozwiązaniach związanych z organizacją w Rzeczypospolitej Polskiej sesji Konferencji Stron Ramowej konwencji Narodów Zjednoczonych w sprawie zmian klimatu* (w zakresie przyznania Służbie Ochrony Państwa analogicznych do Policji uprawnień pozwalających na przetwarzanie danych, co związane jest ze zwiększeniem uprawnień Służby Ochrony Państwa względem Biura Ochrony Rządu), w ustawie z dnia 12 października 1990 r. o Straży Granicznej (w zakresie ujednolicenia z rozwiązaniami przyjętymi w odniesieniu do Policji, a dotyczącymi kwestii pozyskiwania informacji i przetwarzania danych osobowych) zaproponowane w projekcie ustawy zmiany są bezpośrednią konsekwencją wdrożenia rozwiązań wynikających z rozporządzenia 2016/679 oraz dyrektywy 2016/680. Z uwagi na powiązanie treściowe z kwestią przetwarzania danych osobowych w przepisach ustawy o Policji oraz o Straży Granicznej dodano przepisy regulujące rejestrowanie obrazu i dźwięku m.in. podczas interwencji. Określono czas przechowywania uzyskanych w ten sposób informacji, w tym danych osobowych, co stanowić będzie gwarancje, że gromadzone dane nie będą nadmiernie długo i bez potrzeby przetwarzane przez Policję i Straż Graniczną.

W kontekście proponowanej zmiany w ustawie o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412), zwanej dalej „uoin" wskazać należy, iż pojęcia „danych osobowych" nie należy utożsamiać z pojęciem „informacji niejawnych". Danymi osobowymi są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Natomiast informacje niejawne to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne – art. 1 ust. 1 uoin.

Zasady klasyfikowania informacji niejawnych do poszczególnych klauzul tajności określa art. 5 uoin. Dane osobowe i informacje niejawne są dwiema różnymi

kategoriami informacji ustawowo chronionych (zob. też art. 1 ust. 3 uoin), choć ich zakresy w pewnym stopniu mogą się pokrywać. Informacje niejawne, którym nadano określoną klauzulę tajności, mogą być udostępnione wyłącznie osobie uprawnionej zgodnie z przepisami uoin dotyczącymi dostępu do określonej klauzuli tajności, muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie. Dostęp do tych informacji jest zatem ograniczony gdyż, zgodnie z art. 21 uoin, dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej może nastąpić dopiero po uzyskaniu poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych. Jeżeli określone dane stanowią zarówno dane osobowe, jak też informacje niejawne w rozumieniu uoin – zastosowanie w takim przypadku winna znaleźć reguła kolizyjna, która wymaga wyraźnego wyartykułowania w przedmiotowej ustawie.

Dodatkowo należy pamiętać, że organem właściwym w zakresie kontroli ochrony informacji niejawnych jest Agencja Bezpieczeństwa Wewnętrznego (odpowiednio Służba Kontrwywiadu Wojskowego). Do jej zadań należy, m.in. realizacja zadań w zakresie bezpieczeństwa systemów teleinformatycznych, przeznaczonych do przetwarzania informacji niejawnych. Przetwarzanie informacji niejawnych w systemach teleinformatycznych wymaga wdrożenia zaawansowanych rozwiązań organizacyjno-technicznych, m.in. dokumentację bezpieczeństwa systemu teleinformatycznego, tj. dokumentu szczególnych wymagań bezpieczeństwa (SWB) oraz dokumentu procedur bezpiecznej eksploatacji (PBS) systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w uoin. Systemy teleinformatyczne, w których przetwarzane są krajowe informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego, której udziela się na czas określony, nie dłuższy niż 5 lat. Proces udzielania przez Agencję Bezpieczeństwa Wewnętrznego akredytacji bezpieczeństwa teleinformatycznego, którego elementem jest audyt, kończy się wydaniem akredytacji bezpieczeństwa dla każdego stanowiska dostępowego i systemu teleinformatycznego. Prowadzona jest także certyfikacja środków ochrony

elektromagnetycznej, której podlegają urządzenia lub narzędzia służące do realizacji zabezpieczenia teleinformatycznego oraz urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych. Wskazać należy, że *ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* również wprowadza pojęcie certyfikacji, co powoduje swego rodzaju dualizm poznawczy.

Mając powyższe na uwadze, zauważyć należy, iż przepisy ustawy o ochronie informacji niejawnych zapewniają daleko idącą ochronę informacji niejawnych, w tym danych osobowych. Jednocześnie Kodeks karny przewiduje surowe sankcje i określa przestępstwa skierowane przeciwko szeroko rozumianej ochronie informacji. Tym samym za niezbędne należy uznać wprowadzenie rozwiązania rozgraniczającego te dwa reżimy ochrony przez wprowadzenie odpowiednich przepisów w projekcie *ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* oraz odpowiednich zmian w *ustawie o ochronie informacji niejawnych.*

Dyrektywa 2016/680 nie ma zastosowania do czynności podmiotów zajmujących się bezpieczeństwem narodowym (art. 2 ust. 3 lit. a w zw. z motywem 14 dyrektywy), a zatem, w kontekście polskiego systemu prawnego, do służb specjalnych, tj. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego. W związku z powyższym, a także mając na względzie, że analogiczne wyłączenia zostały przewidziane 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 uchylające dyrektywę 95/46/WE, a także w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, powstała potrzeba zmiany ustaw regulujących funkcjonowanie służb specjalnych (ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym) przez wprowadzenie przepisów stanowiących samoistną podstawę przetwarzania danych osobowych przez te podmioty.

Zmiany w ustawie z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przetwarzania danych dotyczących przelotu pasażera (Dz. U. poz. 894) mają na celu

dostosowanie jej przepisów w zakresie ochrony danych osobowych pasażerów lotów PNR do projektowanej regulacji. Wprowadzane zmiany polegają na zastąpieniu odesłań do tracącej moc ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723) odesłaniami do projektowanej ustawy oraz zastąpieniu wyrazów Generalny Inspektor Ochrony Danych Osobowych nową nazwą organu nadzorczego, w rozumieniu art. 41 dyrektywy 2016/680, tj. Prezesa Urzędu Ochrony Danych Osobowych. Utrata mocy przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych powoduje również konieczność dostosowania przewidzianych w zmienianej ustawie warunków przekazania danych PNR do państw trzecich w zakresie wymaganego obowiązującego tam poziomu ochrony danych osobowych. Wdrożona przez zmienianą ustawę dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR). W celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE L 119 z 04.05.2016, str. 132) odsyła w tym zakresie do prawa krajowego przyjętego w ramach wdrożenia art. 13 decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. Urz. UE L 350 z 30.12.2008, str. 60). Warunki przekazania danych osobowych do państw trzecich uregulowane są obecnie przez art. 35–38 dyrektywy 2016/680. Kwestia oceny wymaganego unijnym prawem poziomu ochrony danych osobowych uregulowane zostały w polskim porządku prawnym przez w art. 18b–18d ustawy z dnia o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi, do których to odsyłać będzie zmieniany art. 53 ust. 1 pkt 3. Przewidziany obecnie w art. 53 ust. 2 zmienianej ustawy wyjątek w zakresie możliwości przekazania danych PNR mimo nie zapewnienia przez państwo trzecie odpowiedniego poziomu ochrony przekazywanych danych objęty jest zakresem – stosowanego na podstawie zmienionego art. 53 ust. 1 pkt 3 – art. 18d ustawy z dnia o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi, zatem art. 53 ust. 2 zmienianej.

Ponadto wśród właściwych organów w rozumieniu o przetwarzaniu danych dotyczących przetwarzania danych dotyczących przelotu pasażera rozumianych jako organy uprawnione w Rzeczypospolitej Polskiej do występowania o przekazanie danych PNR lub wyników ich przetwarzania oraz do otrzymywania takich danych i wyników ich przetwarzania, do celów określonych w art. 1 ust. 1 tej ustawy, proponuje się uwzględnienie Komendanta Służby Ochrony Państwa. Do zadań SOP należy bowiem ochrona Prezydenta RP, Marszałka Sejmu, Marszałka Senatu, Prezesa Rady Ministrów, wiceprezesa Rady Ministrów, ministra właściwego do spraw wewnętrznych oraz ministra właściwego do spraw zagranicznych, a także byłych prezydentów RP i innych osób ze względu na dobro państwa wskazanych w decyzji ministra właściwego do spraw wewnętrznych. Realizowane działania ochronne mogą dotyczyć między innymi zabezpieczenia przelotów lotniczych osób chronionych, dlatego też niezbędne jest zapewnienie tej formacji dostępu do danych o pasażerach.

W przypadku gdy w przepisach zmieniających alternatywnie określono administratorów danych osobowych, wydane przez właściwych administratorów akty wewnętrzne, w tym polityki ochrony danych osobowych określą podział zadań między tymi podmiotami.

W ustawach określających zadania i uprawnienia części służb i innych podmiotów objętych regulacją wprowadzono, w ograniczonym zakresie, wyłączenia od stosowania poszczególnych 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. Ograniczenia te znajdują jednak swoje zastosowanie do wąskiej grupy przypadków, jak przetwarzanie danych osobowych w związku z prowadzonymi postępowaniami kwalifikacyjnymi czy przebiegiem stosunku służbowego, w tym po jego ustaniu. Nie wprowadzono zatem blokowych wyłączeń w odniesieniu do art. 12–22 i art. 34 RODO, a pojedyncze ograniczenia skonstruowane w taki sposób, aby zapewnić realizację praw osób wynikających z rozporządzenia, przy zachowaniu poufności stosowanych w tym zakresie procedur oraz z uwzględnieniem obowiązujących ustaw regulujących zasady działania tych formacji. Mając na względzie przedmiotowy zakres projektowanych regulacji, wprowadzono je wyłącznie w zakresie art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia, w zakresie w jakim przepisy szczególne przewidują odrębny tryb sprostowania. W

odniesieniu do określonego w art. 13 RODO obowiązku informacyjnego, wyłączono jedynie jego realizację w odniesieniu do ust. 1 lit d i e, tj. jeżeli 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 oraz przekazywanie informacji o odbiorcach danych osobowych lub o kategoriach odbiorców. Tym samym osoba, której dane dotyczą uzyska informacje o przetwarzaniu jej danych osobowych i w konkretnym przypadku będzie mogła dochodzić swoich praw, w oparciu o określone w art. 15 prawo dostępu. Celem tego ograniczenia jest natomiast możliwość odstąpienia od upowszechnienia informacji dla bliżej nieokreślonego kręgu osób np. przez publikację na stronie internetowej podmiotu lub na stronie podmiotowej BIP możliwych kategorii odbiorców.

Art. 16 rozporządzenia określający prawo do sprostowania nieprawidłowych danych osobowych nie znajdzie zastosowania wyłącznie w przypadku, gdy przepisy szczególne będą przewidywały odrębny tryb sprostowania. Tym samym prawo osoby do sprostowania jej danych osobowych zostanie zachowane. Jednocześnie w celu zapewnienia odpowiedniego poziomu przetwarzanych w ten sposób danych osobowych wskazano, że polega ono co najmniej na dopuszczeniu do ich przetwarzania wyłącznie pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności.

Zrezygnowano natomiast z wyłączenia stosowania art. 14 rozporządzenia, gdyż stosowanie przepisu jest wyłączone z mocy rozporządzenia. Dane pozyskiwane w związku z prowadzonymi postępowaniami kwalifikacyjnymi, jeżeli podlegają udostępnieniu innym administratorom danych, to jedynie w przypadkach wprost przewidzianych przepisami prawa i w związku z realizacją przez te podmioty zadań publicznych. Zgodnie z art. 14 ust. 5 lit. c rozporządzenia przepis ten nie ma zastosowania, jeżeli „pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego”.

Również art. 17 rozporządzenia nie znajdzie zastosowania, gdy jest to konieczne „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". Dane osobowe gromadzone w ramach postępowań kwalifikacyjnych będą przechowywane przez określone w przepisach prawa okresy retencji. Mogą być również gromadzone po upływie tych okresów m.in. z uwagi na potrzebę ochrony przed ewentualnymi roszczeniami kandydatów do służby np. z powodu dyskryminacji. Bez dostępu do dokumentów rekrutacyjnych formacje nie mogłyby się skutecznie bronić przed tego rodzaju zarzutami. Zgodnie z art. 17 ust. 3 lit. e prawo do bycia zapomnianym nie znajdzie zastosowania, gdy jest to konieczne „do ustalenia, dochodzenia lub obrony roszczeń".

W odniesieniu do art. 19 rozporządzenia regulującego kwestię informowania odbiorców np. o sprostowaniu danych osobowych lub ograniczaniu ich przetwarzania, zauważyć należy, że zgodnie z definicją przyjętą w rozporządzeniu, odbiorcami nie są organy publiczne, które otrzymują dane osobowe w ramach postępowania prowadzonego na podstawie przepisów prawa. Ponadto w treści cytowanego artykułu przewidziano możliwość wyłączenia od obowiązku informowania, jeżeli poinformowanie okaże się niemożliwe lub wymaga niewspółmiernie dużego wysiłku.

Artykuł 20 rozporządzenia określający zasadę przenoszalności danych nie znajdzie zastosowania, gdyż zgodnie z motywem (68) rozporządzenia „prawa tego – z uwagi na jego charakter – nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych. Dlatego nie powinien mieć on zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi". Działania podejmowane przez służby są działaniami podejmowanymi w interesie publicznym w ramach sprawowania władzy publicznej. Służby, co do zasady, nie odbierają zgód na przetwarzanie danych osobowych, a postępowanie kwalifikacyjne nie jest wykonaniem umowy. Z tego powodu również w tym zakresie przepis nie znajdzie zastosowania.

W praktyce nie znajdzie zastosowania również przepis art. 21 przewidujący prawo osoby, której dane dotyczą do wniesienia w dowolnym momencie sprzeciwu – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych

przepisów. W przypadku wykonywania zadań przez organy publiczne, które wynikają z przepisów prawa, sprzeciw nie przysługuje lub nie może zostać uwzględniony przez administratora ze względu na podstawę przetwarzania z art. 6 ust. 1 lit. c rozporządzenia.

Przewidziane w przepisach pragmatycznych formacji i służb prawo do przetwarzania danych osobowych bez wiedzy i zgody osób, których dane dotyczą nie stanowi normy kompetencyjnej do wyłączenia korzystania przez osobę, której dane dotyczą z praw określonych w art. 22–25 projektowanej ustawy. Wyłączenia w tym zakresie określone zostały w art. 26 projektu.

W odniesieniu do projektowanego art. 24 ust. 5 pkt 1 ustawy o Służbie Więziennej wyłączającego prawo dostępu osoby pozbawionej wolności do jej akt osobowych prowadzonych przez administrację zakładu karnego lub aresztu śledczego zauważyć należy, że nie wyłącza on prawa tej osoby do uzyskania informacji o przetwarzanych przez administrację zakładu karnego lub aresztu śledczego danych osobowych tej osoby. Ograniczenie dostępu do akt, w których gromadzone są różnego rodzaju informacje o osadzonym, związane jest z koniecznością zapewnienia bezpieczeństwa zarówno innym osadzonym, jak również funkcjonariuszom Służby Więziennej.

W rozdziale 10 zaproponowano przepisy przejściowe, dostosowujące i końcowe.

W projekcie zagwarantowano administratorom odpowiedni czas – na wyznaczenie inspektora ochrony danych. Do tego czasu funkcję tę pełnić będą dotychczasowi administratorzy bezpieczeństwa informacji.

Określono również zasady postępowania w odniesieniu do spraw rozpoczętych i niezakończonych przed wejściem w życie projektowanych przepisów (czynności kontrolne, postępowania wszczęte przez Prezesa Urzędu Ochrony Danych Osobowych), między innymi przez:

- gwarancję ważności i skuteczności wykonanych dotychczas czynności oraz wydanych rozstrzygnięć,
- przyjęcie generalnej zasady stosowania przepisów dotychczasowych,
- postępowania z wnioskami o ponowne rozpatrzenie sprawy i skargami na wykonane dotychczas czynności oraz wydane rozstrzygnięcia.

Projekt zobowiązuje administratora do dostosowania zasad przetwarzania danych osobowych do środków technicznych i organizacyjnych określonych w projekcie

ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Jednocześnie upoważnienia do przetwarzania danych osobowych wydane przed wejściem w życie *ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*, zachowują moc przez okres 12 miesięcy. Natomiast zgody wydane przez służby, instytucje państwowe oraz organy władzy publicznej na udostępnianie za pomocą urządzeń telekomunikacyjnych lub w drodze teletransmisji informacji, w tym danych osobowych, jednostkom organizacyjnym Policji, jednostkom organizacyjnym Straży Granicznej lub Służbie Ochrony Państwa zachowują swoją moc, bez konieczności wydawania ich w trybie nowych przepisów.

W terminie 1 roku od dnia wejścia w życie ustawy administrator dostosuje zasady przetwarzania danych osobowych do środków technicznych i organizacyjnych, o których mowa w art. 39. Jeżeli wymagać to będzie niewspółmiernie dużego wysiłku lub nakładów administrator, będzie mógł dostosować zautomatyzowane systemy przetwarzania danych osobowych do środków technicznych i organizacyjnych, w terminie dłuższym niż wskazano powyżej, nie później jednak niż do dnia 6 maja 2023 r.

Dotychczasowe rozstrzygnięcia określające zasady udostępniania informacji i danych osobowych z Centralnej Bazy Danych Osób Pozbawionych Wolności, za pośrednictwem systemu teleinformatycznego, zachowują moc do dnia wejścia w życie decyzji wydanych na podstawie art. 25d ust. 1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, dodanego niniejszą ustawą, nie dłużej jednak niż przez okres 2 lat od dnia wejścia w życie niniejszej ustawy.

Dostosowanie zasad przetwarzania informacji i danych osobowych w zbiorach danych utworzonych przed dniem wejścia w życie niniejszej ustawy do wymogów, o których mowa w art. 20, art. 21 i art. 36, nastąpi w terminie nie później niż do dnia 6 maja 2023 r.

W rozdziale tym określono także okresy obowiązywania aktów wykonawczych wydanych na podstawie dotychczasowych przepisów ustrojowych podmiotów objętych projektem oraz terminy wejścia niektórych projektowanych przepisów.

Zaproponowano również wdrożenie przepisu określającego mechanizm korygujący odnoszący się do proponowanego w ocenie skutków regulacji zwiększenia środków wydatkowanych z budżetu państwa. Prezes Urzędu Ochrony Danych Osobowych będzie monitorował wykorzystanie limitu wydatków i dokonywał oceny wykorzystania tego limitu według stanu na koniec każdego kwartału. Natomiast w przypadku przekroczenia lub zagrożenia przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków oraz w przypadku, gdy w okresie od początku roku kalendarzowego do dnia ostatniej oceny, część limitu rocznego przypadającego proporcjonalnie na ten okres zostanie przekroczona co najmniej o 10% stosowany będzie mechanizm korygujący polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym niniejszej ustawy. Jako organ właściwy do wdrożenia mechanizmu korygującego wskazano Prezesa Urzędu Ochrony Danych Osobowych.

Wskazano również, że zachowane w mocy przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych w odniesieniu do zagadnień objętych zakresem regulacji projektowanej ustawy w terminie do dnia jej wejścia w życie, stracą moc.

W projekcie wskazano, iż ustawa wejdzie w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem art. 82 pkt 5 w zakresie art. 25c–25h, które wchodzą w życie po upływie roku od dnia ogłoszenia.

Informacje dodatkowe

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz art. 52 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn. zm.) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji. Do Ministra Spraw Wewnętrznych i Administracji nie zgłoszono zainteresowania pracami nad projektem niniejszej ustawy w trybie art. 7 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Zawarte w projekcie ustawy regulacje nie stanowią przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm aktów

prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), w związku z tym projekt ustawy nie będzie podlegał notyfikacji.

Projekt został, zgodnie z § 32 ust. 2 uchwały nr 190 z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów, przekazany do Koordynatora oceny skutków regulacji w Kancelarii Prezesa Rady Ministrów.

Nazwa projektu Projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Spraw Wewnętrznych i Administracji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Krzysztof Kozłowski – Sekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji **Kontakt do opiekuna merytorycznego projektu** Pan Mariusz Cichomski Dyrektor Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji tel. 022 60 140 70 fax. 022 845 18 20 e-mail: dpp.koordynacja@mswia.gov.pl	**Data sporządzenia** **20.08.2018 r.** **Źródło:** Prawo UE Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016, s. 89) **Nr w Wykazie prac: UC116**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Przygotowanie projektu *ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* wynika z konieczności wdrożenia do polskiego porządku prawnego rozwiązań zawartych w dyrektywie 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), zwanej dalej „dyrektywą 2016/680".

Dyrektywa 2016/680 oraz kluczowe dla nowej koncepcji ochrony danych osobowych 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)* (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwane dalej „rozporządzeniem 2016/679", w sposób kompleksowy i spójny dla całej Unii Europejskiej regulują zagadnienia ochrony danych.

Ustawodawca europejski celowo wyłączył z zakresu stosowania rozporządzenia 2016/679 przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, regulując te kwestie – ze względu na szczególny charakter takich czynności – w akcie prawnym innej rangi, to jest dyrektywie 2016/680. Dyrektywa bowiem, jako akt prawny zobowiązujący państwa członkowskie do ustanowienia danego porządku prawnego – w przeciwieństwie do rozporządzenia, którego przepisy mają zastosowanie wprost – pozwala na uwzględnienie w przygotowywanych na jej podstawie przepisach różnorodności i odmienności krajowych regulacji w zakresie zapobiegania i zwalczania przestępczości.

Jednocześnie dyrektywa do organów właściwych – oprócz organów publicznych, takich jak organy sądowe, Policja lub inne organy ścigania – zalicza również wszelkie inne organy lub podmioty, którym prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych w celach określonych w dyrektywie 2016/680.

Kryterium celu przetwarzania jest zatem kluczowe dla ustalenia, czy zastosowanie będzie miała dyrektywa 2016/680, czy rozporządzenie 2016/679. Rozporządzenie 2016/679 ma zastosowanie również wtedy, gdy organ lub podmiot zbiera dane osobowe do innych celów, a następnie dalej te dane przetwarza w celu realizacji obowiązku prawnego, któremu podlega.

Brzmienie dyrektywy 2016/680 zostało jednocześnie skorelowane z tekstem ogólnego rozporządzenia o ochronie

danych w ten sposób, że oba akty prawne bazują na tych samych zasadach ogólnych. Organy ścigania będą musiały zatem w pełni przestrzegać zasad celowości, adekwatności i legalności. Wyrazem tej tendencji jest również możliwość wyznaczenia tych samych organów nadzorczych.

Dyrektywa 2016/680 nie ma zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym, ani przetwarzania danych osobowych przez państwa członkowskie podczas czynności, które wchodzą w zakres zastosowania tytułu V rozdziału 2 Traktatu o Unii Europejskiej, nie wchodzą w zakres dyrektywy.

Dyrektywa 2016/680 reguluje również kwestie wymiany informacji obejmujących dane osobowe między organami ścigania państw członkowskich oraz państwami trzecimi. Obowiązujące dotychczas w tym obszarze regulacje, w postaci uchylanej dyrektywy 95/46/WE Parlamentu Europejskiego i Rady miały wprawdzie zastosowanie do całości przetwarzania danych osobowych w ramach państw członkowskich, zarówno w sektorze publicznym, jak i prywatnym. Nie miały jednak zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty", takiej jak działania w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Podobnie uchylana decyzja ramowa Rady 2008/977/WSiSW miała zastosowanie do współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej ograniczonej do przetwarzania danych osobowych przesyłanych lub udostępnianych wyłącznie pomiędzy państwami członkowskimi. Regulacje te okazały się niewystarczające w związku z dynamicznym rozwojem przestępczości o charakterze transgranicznym i międzynarodowym, będącym w znacznej mierze wynikiem postępu technologicznego w zakresie wymiany informacji.

Mając na uwadze powyższe konieczne było przygotowanie nowego aktu prawnego, który w sposób kompleksowy wdroży do polskiego porządku prawnego rozwiązania zawarte w dyrektywie 2016/680. Zaproponowane w projekcie rozwiązania stanowią realizację nałożonego na państwa członkowskie w art. 63 dyrektywy 2016/680 obowiązku transpozycji jej przepisów do krajowego porządku prawnego.

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

Projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i przeciwdziałaniem przestępczości określa dopuszczalne cele przetwarzania danych osobowych w rozumieniu ustawy, zakres przedmiotowy i podmiotowy tego aktu prawnego, definicję danych osobowych oraz wyjaśnienie innych, stosowanych w ustawie pojęć, wywodzących się z dyrektywy 2016/680. Projektowane przepisy określają również zadania organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – który jest tożsamy z organem nadzorczym określonym w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, a realizującym zadania nadzorcze wynikające z rozporządzenia 2016/679. Pomimo tego zadania i uprawnienia organu, nadzorczego określone w tej części projektowanych przepisów, uwzględniają odmienność celów przetwarzania danych osobowych wynikających z dyrektywy 2016/680.

Projektowane przepisy zawierają również regulacje w zakresie zasad przetwarzania danych osobowych oraz praw osób, których dane dotyczą, określają również zadania i wymogi stawiane przed administratorem, podmiotem przetwarzającym oraz inspektorem ochrony danych osobowych. W projekcie ujęte są również kwestie współpracy Prezesa Urzędu Ochrony Danych Osobowych z organami nadzorczymi innych państw Unii Europejskiej, a także środków ochrony prawnej przysługujących osobom, których dane są przetrwane. Uwzględnione zostały również przepisy zmieniające inne ustawy w zakresie niezbędnym do implementacji przepisów wynikających z dyrektywy 2016/680 oraz przepisy przejściowe, dostosowujące i końcowe.

Zakres przedmiotowy i podmiotowy oraz cele przetwarzania danych osobowych.

Dane osobowe w rozumieniu projektu ustawy mogą być przetwarzane w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności. Projekt ustawy określa również prawa osób, których dane osobowe są przetwarzane oraz środki ochrony prawnej przysługujące tym osobom; sposób prowadzenia nadzoru nad ochroną danych osobowych; zadania organu nadzorczego oraz formy i sposób ich wykonania; obowiązki administratora i podmiotu przetwarzającego oraz inspektora ochrony danych i tryb jego wyznaczania; sposób zabezpieczenia danych osobowych; tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej oraz odpowiedzialność karną za naruszenie przepisów niniejszej ustawy.

W projekcie nie zdecydowano się na skatalogowanie podmiotów, których ustawa dotyczy. Czynnikiem determinującym stosowanie przepisów projektowanej ustawy będą natomiast kompetencje podmiotu określone w regulacjach prawnych rangi ustawy. Powyższa konstrukcja projektowanych przepisów jest przede wszystkim wynikiem wielości podmiotów funkcjonujących w sferze określonej ramami zakresu podmiotowego dyrektywy 2016/680. Rozwiązanie takie jest przy tym na tyle uniwersalne, że w przypadku utworzenia, likwidacji lub przekształcenia działających w tym obszarze podmiotów, nie będzie skutkowało koniecznością wprowadzania zmian

w projektowanych przepisach.

W projekcie wskazano również wyłączenia w odniesieniu do zakresu przedmiotowego ustawy. Zgodnie z nim przepisów ustawy nie stosuje się do ochrony danych osobowych:

1) znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2016 r. poz. 1654 oraz z 2017 r. poz. 773), ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652), ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2017 r. poz. 1904, 2405 oraz z 2018 r. poz. 5, 106, 138 i 201), ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2017 r. poz. 2226 oraz 2018 r. poz. 201), ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475), ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396 oraz z 2016 r. poz. 2205), ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5) oraz wydanych na ich podstawie aktów wykonawczych;
2) przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego.

Z zakresu nadzoru określonego w projektowanych przepisach, kierując się wyjaśnieniem zawartym w motywie (80) dyrektywy 2016/680, wyłączono dane osobowe przetwarzane przez prokuraturę i sądy w toku sprawowania przez nie wymiaru sprawiedliwości. W tym wypadku stosowane będą przepisy szczególne, regulujące ochronę danych osobowych przetwarzanych w ramach prowadzonych postępowań lub wykonywanych czynności, obejmujące zarówno prawodawstwo krajowe (m.in. z zakresu prawa karnego oraz karnego wykonawczego).

Ze stosowania przepisów projektowanej ustawy wyłączono sferę bezpieczeństwa narodowego, w tym – z perspektywy instytucjonalnej – służby specjalne, to jest Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne. Należy podkreślić, że dyrektywa 2016/680 w art. 2 ust. 3 lit a oraz motywie (14) zakłada takie rozwiązanie, stanowiąc, że jej przepisy nie powinny mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym, ani przetwarzania danych osobowych przez państwa członkowskie podczas czynności, które wchodzą w zakres zastosowania tytułu V rozdziału 2 Traktatu o Unii Europejskiej, nie należy uznawać za czynności wchodzące w zakres dyrektywy 2016/680. Ponadto przywołany Traktat o Unii Europejskiej w art. 4 ust. 2 (zdanie trzecie) stanowi, że w szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego.

Nadzór nad przetwarzaniem danych osobowych.

Zgodnie z projektowanymi przepisami funkcję organu nadzorczego w ramach dyrektywy 2016/680 pełnić będzie Prezes Urzędu Ochrony Danych Osobowych (dalej zwany „Prezesem Urzędu" lub „organem nadzorczym"), powołany na podstawie przepisów rozporządzenia 2016/679. Skorzystano w tym przypadku z przewidzianej w art. 41 ust. 3 dyrektywy 2016/680 możliwości, aby organem tym był organ nadzorczy ustanowiony na mocy rozporządzenia 2016/679. Rozwiązanie to jest korzystne nie tylko ze względów ekonomicznych (nie ma potrzeby tworzenia odrębnego urzędu), ale przede wszystkim gwarantuje spójność systemu ochrony danych osobowych, a przez to ich większe bezpieczeństwo. W ten sposób zapewniono również niezależność organu nadzorczego, stanowiącą nieodzowny element całego systemu. (W odniesieniu do sądów i prokuratury określono natomiast w przepisach zmieniających inne ustawy oddzielne organy nadzorcze gwarantujące zachowanie statusu niezależności sądów i prokuratury).

Z uwagi na podobny sposób określenia niektórych zadań organu nadzorczego w rozporządzeniu 2016/679 oraz dyrektywie 2016/680, a także ze względu na to, że ustanowiony będzie jeden wspólny organ nadzorczy dla tych dwóch reżimów prawnych, w projektowanych przepisach skupiono się na zadaniach Prezesa Urzędu, wynikających ze specyfiki przetwarzania danych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar. Mając na uwadze powyższe, wśród zadań Prezesa Urzędu wskazano m.in.: monitorowanie i egzekwowanie stosowania przepisów niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych; upowszechnianie wiedzy z zakresu stosowania niniejszej ustawy, w szczególności wśród administratorów i podmiotów przetwarzających; sprawdzanie zgodności przetwarzania danych osobowych z przepisami niniejszej ustawy w przypadku, gdy administrator, na podstawie przepisów ustawy, odmówił udzielenia informacji oraz informowanie osoby, której dane dotyczą, o wynikach tego sprawdzenia lub o powodach jej nieprzeprowadzenia; pełnienie funkcji konsultacyjnych, dotyczących operacji przetwarzania w ramach niniejszej projektowanej ustawy.

Prezes Urzędu dysponować będzie również możliwością przeprowadzania kontroli przetwarzania danych osobowych, wykorzystując w tym celu procedury uregulowane w rozdziale 9 ustawy z ustawie z dnia 10 maja 2018 r. o ochronie

danych osobowych. Rozwiązanie to stanowi dodatkowy element gwarancyjny w maksymalny sposób zbliżający oba systemy ochrony danych osobowych, ale uwzględniający jednocześnie ich specyfikę.

Kierując się wspomnianą specyfiką określono, również uprawnienia kontrolującego, który w toku kontroli ma prawo wglądu do zbioru zawierającego dane osobowe, z zachowaniem przepisów ustawy o ochronie informacji niejawnych, jedynie w obecności upoważnionego przedstawiciela właściwego organu, w którym jest przeprowadzana kontrola. Z kolei podmioty kontrolowane (administrator, podmiot przetwarzający lub odbiorca) są obowiązane umożliwić kontrolującemu przeprowadzenie kontroli.

Zgodnie z projektowanymi przepisami w przypadku naruszenia przepisów o ochronie danych osobowych, Prezes Urzędu w drodze decyzji administracyjnej, nakazuje administratorowi lub podmiotowi przetwarzającemu przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień;
2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;
3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;
4) zabezpieczenie danych osobowych lub przekazanie ich innym podmiotom;
5) usunięcie danych osobowych;
6) wprowadzenie czasowych lub stałych ograniczeń przetwarzania i przekazywania, w tym zakazu przetwarzania.

Jednocześnie powyższa decyzja Prezesa Urzędu nie może nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Administrator, w przypadku uznania, że zgromadzone w ten sposób dane są zbędne, jest zobowiązany do ich usunięcia. W przypadku niedopełnienia obowiązku usunięcia danych osobowych przez administratora Prezes Urzędu może nakazać ich usunięcie. W celu realizacji uprawnienia Prezes Urzędu nie uzyskuje dostępu do danych osobowych zgromadzonych w toku tych czynności (art. 8 ust. 3). Z uwagi na specyficzny, a także niejawny charakter tego rodzaju czynności, przepis ten umożliwia dalsze przetwarzanie danych uzyskanych z naruszeniem przepisów projektowanej ustawy. Rozwiązanie to nie wyłącza jednak możliwości skorzystania przez organ nadzorczy z pozostałych mechanizmów gwarancyjnych. Ponadto administrator lub podmiot przetwarzający będzie zobowiązany, bez zbędnej zwłoki, do przywrócenia zgodnego z prawem sposobu przetwarzania danych osobowych.

Dodatkowo przewidziano możliwość wystąpienia przez Prezesa Urzędu bezpośrednio do inspektora danych osobowych o dokonanie sprawdzenia stosowania przepisów projektowanej ustawy przez administratora, który tego inspektora powołał. Jednocześnie przeprowadzenie tego rodzaju sprawdzenia nie wyłącza prawa Prezesa Urzędu do przeprowadzenia przez niego kontroli.

W projekcie ustawy przyjęto rozwiązanie, zgodnie z którym do prowadzonych na jej podstawie postępowań stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257, z późn. zm.), o ile przepisy projektowanej ustawy nie stanowią inaczej. Decyzje Prezesa Urzędu podlegają z kolei zaskarżeniu do sądu administracyjnego.

Zasady przetwarzania danych osobowych.

Oprócz ogólnych przepisów odnoszących się do konieczności przestrzegania przepisów prawa oraz zgodności z celami przetwarzania danych, określonymi w projektowanej ustawie, w projektowanych przepisach przewidziano również sytuację, gdy dane zebrane pierwotnie w jednym z przewidzianych przez ustawę celów będą przetwarzane w innym, ale również przewidzianym przez tę ustawę, celu.

Projektowana ustawa, co do zasady, zabrania przetwarzania danych osobowych, określanych jako wrażliwe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko naruszenia podstawowych praw i wolności. Chodzi przede wszystkim o dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej.

Mając jednakże na uwadze wytyczne sformułowane w motywach (37) i (51) oraz w art. 10 dyrektywy 2016/680, przetwarzanie tego rodzaju danych, na zasadzie wyjątku dopuszczono, jeżeli jest to niezbędne dla osiągnięcia prawnie dopuszczalnych celów określonych w odrębnych przepisach, ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby albo dane takie zostały upublicznione przez osobę, której dane dotyczą. W projektowanych przepisach zagwarantowano, aby ostateczne rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, mające dla niej niekorzystne skutki prawne lub poważnie na nią wpływające, nie były podejmowane wyłącznie w wyniku przetwarzania danych osobowych w sposób zautomatyzowany, w tym w wyniku profilowania, chyba że dopuszcza je prawo Unii Europejskiej lub odrębne przepisy, którym podlega administrator i które przewidują odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą. Minimum wymaganym w takich przypadkach to

możliwość uzyskania interwencji ze strony administratora. Projektowana ustawa zabrania również, aby rozstrzygnięcia takie podejmowane były na podstawie danych wrażliwych, które nie mogą być również wykorzystywane do profilowania osób fizycznych.

Projektowane przepisy nakładają na administratorów obowiązek weryfikacji w terminach określonych przez przepisy szczególne, regulujące działania właściwego organu, a jeśli przepisy te nie określają terminu – nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych. Weryfikacja będzie dokonywana w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane będą usuwane. Wprowadzenie powyższego przepisu stanowi realizację dyspozycji art. 5 dyrektywy 2016/680 obligującego do przyjęcia odpowiednich terminów usuwania danych osobowych lub okresowego przeglądu konieczności ich przechowywania. Jednocześnie w projekcie ustawy przewidziano, że dane osobowe uznane za zbędne można przekształcić w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań.

Kierując się treścią motywu (31), zgodnie z którym w stosownych przypadkach należy w jak największym stopniu wyraźnie rozróżniać dane osobowe różnych kategorii osób, których dane dotyczą, a także w oparciu o sposób sformułowania art. 6 dyrektywy 2016/680, w projekcie zaproponowano, aby o ile rozróżnienie to nie jest niemożliwe lub dalece utrudnione, administrator zapewniał podział na dane osobowe dotyczące:

1) osób, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
2) osób skazanych za czyn zabroniony;
3) pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;
4) innych osób związanych z czynem zabronionym, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w ramach postępowania przygotowawczego w sprawie czynu zabronionego lub na dalszych etapach postępowania karnego, osób, które mogą dostarczyć informacji o czynach zabronionych, lub osób, które mają kontakty lub powiązania z jedną z osób, o których mowa w pkt 1 i 2.

Realizując dyspozycję art. 7 dyrektywy 2016/680, który zobowiązuje państwa członkowskie do zapewnienia, by dane osobowe oparte na faktach były rozróżniane, tak dalece, jak to możliwe, z danymi osobowymi opartymi na indywidualnych ocenach, w projekcie ustawy wprowadzono odpowiedni przepis nakładający ten obowiązek na administratorów, z wyłączeniem przypadków, gdy dokonanie takiego rozróżnienia jest niemożliwe lub utrudnione.

Projektowane przepisy umożliwiają również przesyłanie lub udostępnianie danych osobowych innym właściwym organom, państwu trzeciemu lub organizacji międzynarodowej. Właściwy organ będzie mógł przesyłać lub udostępniać dane osobowe innym właściwym organom, państwu trzeciemu lub organizacji międzynarodowej po uprzednim zweryfikowaniu, w miarę potrzeby i możliwości, prawidłowości, kompletności i aktualności tych danych. Właściwy organ, przesyłając dane osobowe odbiorcom, przekazywać będzie także, w miarę potrzeby i możliwości, niezbędne dodatkowe informacje pozwalające odbiorcy ocenić stopień prawidłowości, kompletności oraz aktualności przesłanych danych osobowych.

Prawa osoby, której dane dotyczą.

W art. 24 określony został obowiązek informacyjny realizowany przez administratora, przy czym ust. 1 i 3 stanowią implementację obowiązku informacyjnego wynikającego z art. 13 ust. 1–2 dyrektywy, zaś ust. 4 – obowiązku informacyjnego określonego w art. 14 dyrektywy. Mając na względzie, że przepisy dyrektywy odmiennie określają charakter tego obowiązku w każdym z cytowanych artykułów, w projekcie określono, że obowiązek wynikający z ust. 1 i 3 realizowany jest przez administratora z urzędu, zaś określony w ust. 4 – na wniosek osoby, której dane dotyczą. W projekcie określono również prawo osoby, której dane dotyczą, do dostępu do jej danych osobowych (art. 23 ust. 1), przy czym prawo to zostało określone jako udostępnienie lub przekazanie wnioskodawcy kopii danych osobowych albo sporządzonego w przystępnej formie wyciągu z tych danych (ust. 2). Tak zdefiniowane prawo dostępu jest zgodne z wyjaśnieniem zawartym w motywie (43) preambuły dyrektywy. Zgodnie z art. 24 ust. 1 osoba, której dane dotyczą, może wystąpić do administratora z wnioskiem o:

1) uzupełnienie, uaktualnienie lub sprostowanie danych osobowych – w przypadku, gdy dane te są niekompletne, nieaktualne lub nieprawdziwe;
2) usunięcie danych osobowych – w przypadku, gdy dane te zostały zebrane lub są przetwarzane z naruszeniem przepisów niniejszej ustawy.

W przypadku stwierdzenia, że dane są niekompletne, nieaktualne lub nieprawdziwe, administrator dokonuje ich usunięcia z urzędu. Jeżeli wniosek o sprostowanie lub uaktualnienie dotyczy danych, które znajdują się również w dokumencie zawierającym zeznanie, wypowiedź czy oświadczenie osoby fizycznej, a ustalono, że dane te są nieprawdziwe lub nieaktualne, administrator pozostawia je w postaci niezmienionej. Wniosek taki uwzględnia się tylko

poprzez umieszczenie w zbiorze danych stosownej adnotacji (art. 24 ust. 3). Reguła określona w ust. 3 jest zgodna z wyjaśnieniem zawartym w motywie (30 i 47) preambuły dyrektywy.

Od generalnych uprawnień przewiduje się jednak niezbędne wyłączenia. Nie będą przekazywane informacje, jeżeli mogłoby to powodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karno- skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
4) zagrożenie dla życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
5) zagrożenie dla bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
6) istotne naruszenie dóbr osobistych innych osób.

Jednak administrator będzie mógł przekazać osobie, której dane dotyczą, informacje, o których mowa powyżej, w przypadku, gdy ich ujawnienie byłoby niezbędne do ochrony życia lub zdrowia ludzkiego.

Administrator będzie podejmować działania mające na celu ułatwienie osobie, której dane dotyczą, wykonywanie przysługujących jej praw, a także udzielać informacji jasnym i prostym językiem, w takiej samej postaci, w jakiej wniesiono wniosek, chyba że udzielenie informacji w takiej postaci powodowałoby nadmierne trudności lub koszty, lub przepis niniejszej ustawy stanowi inaczej.

Komunikacja prowadzona przez administratora z osobą będzie wolna od opłat. Jeżeli jednak żądania osoby, której dane dotyczą, będą nieuzasadnione lub nadmierne, zwłaszcza ze względu na ich powtarzalność, administrator będzie mógł pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań.

Administrator i podmiot przetwarzający.

Zgodnie z zaproponowanymi w projekcie rozwiązaniami administrator odpowiedzialny jest przede wszystkim za zapewnienie, aby dane osobowe były:

1) przetwarzane zgodne z prawem i rzetelne oraz przy zastosowaniu niezbędnych środków technicznych i organizacyjnych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
2) zbierane i przetwarzane w konkretnych, wyraźnych i uzasadnionych celach;
3) adekwatne do celów, dla których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;
5) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;
6) 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 środków technicznych lub organizacyjnych.

Jednocześnie mając na uwadze treść art. 19 ust. 2 dyrektywy 2016/680, w projektowanych przepisach zobowiązano administratora do opracowania i wdrożenia polityki ochrony danych, uwzględniając w niej sposób dokumentowania środków technicznych i organizacyjnych stosowanych do zapewnienia ochrony danych osobowych, w tym w aspekcie dostępu do danych, wprowadzania danych oraz ich usuwania i weryfikacji, zapewnienia niezawodności i integralności systemów, w których przetwarzane są dane, a w przypadku ich awarii – możliwości odzyskania danych.

Jednym z nowych rozwiązań przewidzianych przez dyrektywę 2016/680, które zostało wprowadzone w projekcie niniejszej ustawy, jest zobowiązanie administratora, aby już w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, planował zastosowanie odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja, a jednocześnie chronił prawa osób, których dane dotyczą. Jeżeli kilku administratorów wspólnie ustali cel i sposoby przetwarzania danych osobowych stają się oni współadministratorami, a ustawa określa mechanizmy podziału zadań między nimi. Administrator może również w drodze pisemnej umowy powierzyć przetwarzanie danych innemu podmiotowi, czyli tzw. podmiotowi przetwarzającemu. Rozwiązanie to zawiera instrumenty gwarancyjne niepozwalające na obniżenie standardu ochrony danych w tego rodzaju sytuacjach. Zawarte w projektowanych przepisach obowiązki podmiotu przetwarzającego wobec administratora stanowią z jednej strony gwarancję, że będzie on wykonywał swoje zadania zgodnie z przepisami projektowanej ustawy, z drugiej zaś zapewniają administratorowi kontrolę nad działaniami tego podmiotu, między innymi poprzez zobowiązanie udostępniania administratorowi wszelkich informacji związanych z weryfikację prawidłowości realizacji umowy powierzenia. Generalnie bowiem odpowiedzialność za przestrzeganie przepisów projektowanej ustawy spoczywa na

administratorze, co nie wyłącza odpowiedzialności podmiotu przetwarzającego za przetwarzanie danych niezgodnie z umową.

W celu zapewnienia rozliczalności w zakresie przetwarzania danych osobowych, na podstawie projektowanych przepisów, administrator oraz podmiot przetwarzający (w powierzonym zakresie) prowadzą wykaz kategorii czynności przetwarzania obejmujący: dane administratora, współadministratora, inspektora ochrony oraz podmiotu przetwarzającego; cele przetwarzania; kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych; opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych; informacje o stosowaniu profilowania – w przypadku gdy zostało ono zastosowane; kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło; wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone; planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe; ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Dyrektywa 2016/680 w motywie (57) oraz art. 25 ust. 1 wprowadziła obowiązek ewidencjonowania operacji przeprowadzanych w zautomatyzowanych systemach przetwarzania, takich jak zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie lub usuwanie danych. Obowiązek ten został wprowadzony również w projektowanych przepisach, w których określono również zgodne z dyrektywą 2016/680 cele prowadzenia powyższej ewidencji, a także obowiązek jej udostępniania organowi nadzorczemu.

Nowością wynikającą z dyrektywy 2016/680 jest również obowiązek dokonania wcześniejszej oceny skutków planowanych operacji przetwarzania przez administratora, jeżeli jakiś rodzaj przetwarzania może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych, a także wprowadzenie uprzednich konsultacji z organem nadzorczym, które mają zagwarantować, że utworzenie nowych zbiorów danych będzie zgodne z przepisami projektowanej ustawy oraz przy wykorzystaniu odpowiednich zabezpieczeń, a także odpowiednio wczesną interwencję organu nadzorczego.

W celu zapewnienia odpowiedniego bezpieczeństwa przetwarzanych danych osobowych administrator lub podmiot przetwarzający mają obowiązek stosować środki techniczne i organizacyjne zapewniające odpowiednią ochronę tych operacji. Temu samemu celowi służy dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie nadane przez administratora lub podmiot przetwarzający. Obowiązek prowadzenia wykazu takich osób spoczywa na administratorze.

Zgodnie z projektowanymi przepisami w przypadkach naruszenia ochrony danych osobowych administrator, bez zbędnej zwłoki, nie później jednak niż w ciągu 72 godzin po stwierdzeniu naruszenia, będzie zgłaszał naruszenie Prezesowi Urzędu, chyba że nie wystąpiło ryzyko naruszenia praw i wolności osób fizycznych. W przypadku niedotrzymania terminu administrator niezwłocznie będzie zgłaszał naruszenie oraz sporządzał i przekazywał Prezesowi Urzędu uzasadnienie niedotrzymania tego terminu. Podmiot przetwarzający – po stwierdzeniu naruszenia ochrony danych osobowych – będzie zgłaszał je administratorowi, bez zbędnej zwłoki, nie później jednak niż w ciągu 48 godzin.

W ramach realizacji wytycznych dyrektywy 2016/680 projekt ustawy przewiduje także dla administratora obowiązek wyznaczenia inspektora ochrony danych. Zgodnie z wyjaśnieniem zawartym w motywie (63) dyrektywy 2016/680 inspektor ochrony danych pomaga administratorowi w monitorowaniu wewnętrznego przestrzegania przepisów przyjętych na podstawie dyrektywy. Osoba ta może być członkiem dotychczasowego personelu administratora. Projektowane przepisy dopuszczają również, że kilku administratorów może, uwzględniając swoją strukturę organizacyjną i wielkość, wspólnie wyznaczyć jednego inspektora ochrony danych, na przykład w przypadku dzielonych zasobów w jednostkach centralnych. Osoba ta może być również mianowana na różne stanowiska w ramach struktury poszczególnych administratorów. Inspektor ochrony danych pomaga również pracownikom przetwarzającym dane osobowe, dostarczając im informacji i porad na temat przestrzegania spoczywających na nich obowiązków w zakresie ochrony danych.

Mając na uwadze szczególną rolę, jaką będzie pełnił inspektor w systemie ochrony danych osobowych, funkcję tę pełnić może osoba, która ukończyła studia wyższe; ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych; posiada odpowiednią wiedzę i doświadczenie zawodowe w zakresie ochrony danych osobowych oraz nie była skazana prawomocnym wyrokiem, orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej. Rozliczenie działalności inspektora następuje na podstawie składanego raz w roku sprawozdania.

Środki ochrony prawnej oraz odpowiedzialność prawna.

Podstawowym prawem osoby, której prawa zostały naruszone w wyniku przetwarzania danych osobowych, jest prawo wniesienia skargi do Prezesa Urzędu. Prawo to przysługiwać będzie w terminie 30 dni od powzięcia wiadomości o tym naruszeniu lub otrzymania informacji od administratora, a Prezes Urzędu udzieli osobie, która wniosła skargę, pomocy prawnej na jej wniosek do czasu rozpatrzenia skargi przez Prezesa Urzędu. Skargę będzie można wnieść za pomocą formularza zamieszczonego na stronie internetowej Prezesa Urzędu, pisemnie, faxem, elektronicznie lub za pomocą elektronicznej platformy usług administracji publicznej ePUAP. Prawo do zgłoszenia naruszenia przetwarzania danych

osobowych przysługiwać będzie również innym osobom, w przypadku powzięcia przez nie wiarygodnej wiadomości o tym naruszeniu. Do rozpatrywania zgłoszeń zastosowanie będzie miał odpowiednio art. 225, art. 231 oraz art. 237–239 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

Na decyzję Prezes Urzędu przysługiwać będzie prawo do wniesienia na tę decyzję skargi do sądu administracyjnego.

Osoba, której dane dotyczą, będzie mogła umocować organizację społeczną o charakterze niezarobkowym, prowadzącą działalność statutową w interesie publicznym i działającą w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych – do wykonywania w jej imieniu praw, w tym wnoszenia środków zaskarżenia, określonych w niniejszym rozdziale.

Natomiast osobie, która poniosła szkodę lub doznała krzywdy w wyniku czynności naruszającej przepisy niniejszej ustawy, przysługiwać będzie od administratora odszkodowanie lub zadośćuczynienie.

Przepisy karne.

W projekcie zaproponowano przepisy karne, zgodnie z którymi 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. Jeśli czyn ten dotyczy danych sensytywnych, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Natomiast kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat dwóch.

Powyższe przepisy karne są dostosowane do przepisów karnych ustawy wdrażającej do polskiego porządku prawnego rozporządzenie 2016/679.

Przepisy zmieniające.

Transpozycja do polskiego prawa dyrektywy 2016/680 wymaga również dokonania odpowiednich zmian w przepisach ustrojowych właściwych organów w sferze zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, a także zmian w innych przepisach odnoszących się do udostępniania danych tym organom. Przepisy normujące niniejsze zagadnienie znalazły się w rozdziale 9 ustawy.

W ramach dostosowania przepisów polskiego prawa do rozwiązań zawartych w dyrektywie 2016/680 zmienia się: ustawę z dnia 26 marca 1982 r. o Trybunale Stanu, ustawę z dnia 18 kwietnia 1985 r. o rybactwie śródlądowym, ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, ustawę z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska, ustawę z dnia 28 września 1991 r. o lasach, ustawę z dnia 13 października 1995 r. Prawo łowieckie, ustawę z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, ustawę z dnia 10 kwietnia 1997 r. – Prawo energetyczne, ustawę z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy, ustawę z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych, ustawę z dnia 29 sierpnia 1997 r. o strażach gminnych, ustawę z dnia 21 grudnia 2000 r. o żegludze śródlądowej, ustawę z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, ustawę z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 6 września 2001 r. o transporcie drogowym, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych, ustawę z dnia 28 marca 2003 r. o transporcie kolejowym, ustawę z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, ustawę z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, ustawę z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, ustawę z dnia 9 kwietnia 2010 r. o Służbie Więziennej, ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, ustawę z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, ustawę z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym, ustawę z dnia 28 stycznia 2016 r. Prawo o prokuraturze, 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 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym, ustawę z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami, ustawę z dnia 8 grudnia 2017 r. o Sądzie Najwyższym, ustawę z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, ustawę z dnia 10 stycznia 2018 r. o szczególnych rozwiązaniach związanych z organizacją w Rzeczypospolitej Polskiej sesji Konferencji Stron Ramowej konwencji Narodów Zjednoczonych w sprawie zmian klimatu, ustawę z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej, ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ustawę z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących

przelotu pasażera.

Przepisy przejściowe, dostosowujące i końcowe.

W projekcie zagwarantowano administratorom odpowiedni czas na wyznaczenie inspektora ochrony danych. Do tego czasu funkcję tę pełnić będą dotychczasowi administratorzy bezpieczeństwa informacji.

Określono również zasady postępowania w odniesieniu do spraw rozpoczętych i niezakończonych przed wejściem w życie projektowanych przepisów.

Jednocześnie upoważnienia do przetwarzania danych osobowych wydane przed wejściem w życie *ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*, zachowują moc przez okres 12 miesięcy. Natomiast zgody wydane przez służby, instytucje państwowe oraz organy władzy publicznej na udostępnianie za pomocą urządzeń telekomunikacyjnych lub w drodze teletransmisji informacji, w tym danych osobowych, jednostkom organizacyjnym Policji lub jednostkom organizacyjnym Straży Granicznej zachowują swoją moc, bez konieczności wydawania ich w trybie nowych przepisów.

W terminie 1 roku od dnia wejścia w życie ustawy administrator dostosuje zasady przetwarzania danych osobowych do środków technicznych i organizacyjnych, o których mowa w art. 39. Jeżeli wymagać to będzie niewspółmiernie dużego wysiłku administrator będzie mógł dostosować zautomatyzowane systemy przetwarzania danych osobowych do środków technicznych i organizacyjnych, w terminie dłuższym niż wskazany powyżej, nie później jednak niż do dnia 6 maja 2023 r.

Dotychczasowe rozstrzygnięcia określające zasady udostępniania informacji i danych osobowych z Centralnej Bazy Danych Osób Pozbawionych Wolności za pośrednictwem systemu teleinformatycznego zachowują moc do dnia wejścia w życie decyzji wydanych na podstawie art. 25d ust. 1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, dodanego niniejszą ustawą, nie dłużej jednak niż przez okres 2 lat od dnia wejścia w życie niniejszej ustawy.

Dostosowanie zasad przetwarzania informacji i danych osobowych w zbiorach danych utworzonych przed dniem wejścia w życie niniejszej ustawy do wymogów, o których mowa w art. 20, art. 21 i art. 36, nastąpi w terminie nie później niż do dnia 6 maja 2023 r.

W rozdziale tym określono także okresy obowiązywania aktów wykonawczych wydanych na podstawie dotychczasowych przepisów ustrojowych podmiotów objętych projektem oraz terminy wejścia niektórych projektowanych przepisów.

Zaproponowano również wdrożenie przepisu określającego mechanizm korygujący, odnoszący się do proponowanego w Ocenie Skutków Regulacji zwiększenia środków wydatkowanych z budżetu państwa. Prezes Urzędu Ochrony Danych Osobowych będzie monitorował wykorzystanie limitu wydatków i dokonywał oceny wykorzystania tego limitu według stanu na koniec każdego kwartału. Natomiast w przypadku przekroczenia lub zagrożenia przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków oraz w przypadku, gdy w okresie od początku roku kalendarzowego do dnia ostatniej oceny część limitu rocznego przypadającego proporcjonalnie na ten okres zostanie przekroczona co najmniej o 10%, stosowany będzie mechanizm korygujący, polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym niniejszej ustawy. Jako organ właściwy do wdrożenia mechanizmu korygującego wskazano Prezesa Urzędu Ochrony Danych Osobowych.

W projekcie wskazano, że ustawa wejdzie w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem art. 82 pkt 5 w zakresie art. 25c–25h, które wchodzą w życie po upływie roku od dnia ogłoszenia.

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

Z dostępnych informacji wynika, że kompleksowe uregulowania krajowe implementujące postanowienia dyrektywy 2016/680 przyjęte zostały jedynie w części państw objętych zakresem stosowania Dyrektywy. Przykładowo w Niemczech– *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680* – stanowi wdrożenie obu elementów pakietu reformującego unijne zasady ochrony danych osobowych.

W części stanowiącej transpozycję dyrektywy 2016/680 niemiecka ustawa w znacznej części powiela przepisy dyrektywy, dostosowane do krajowej prawnej siatki pojęciowej.

Niemiecka ustawa nie zawiera również zmian w przepisach sektorowych, które będą procedowane przez rząd niemiecki na późniejszym etapie.

Obowiązujące w innych państwach regulacje dostosowane są do specyfiki poszczególnych systemów prawnych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Prezes Urzędu Ochrony Danych Osobowych			Ustawa nakłada na Prezesa Urzędu szereg obowiązków

			nadzorczych związanych z ochroną danych osobowych 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.
Policja			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Straż Graniczna			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Żandarmeria Wojskowa			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Krajowa Administracja Skarbowa			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Biuro Nadzoru Wewnętrznego (BNW)			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym

			celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Służba Ochrony Państwa (SOP)			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Powszechne jednostki organizacyjne prokuratury			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Sądy powszechne i wojskowe			Określenie nowych ram prawnych nadzoru nad przetwarzaniem danych osobowych.
Trybunał Konstytucyjny			Określenie nowych ram prawnych nadzoru nad przetwarzaniem danych osobowych.
Sąd Najwyższy			Określenie nowych ram prawnych nadzoru nad przetwarzaniem danych osobowych.
Trybunał Stanu			Określenie nowych ram prawnych nadzoru nad przetwarzaniem danych osobowych.
Straże gminne (miejskie)			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Straż Marszałkowska			Określenie nowych ram prawnych przetwarzania

			danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Służba Więzienna			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Agencja Bezpieczeństwa Wewnętrznego			Aktualizacja odesłań w ustawie pragmatycznej do przepisów stanowiących samoistną podstawę przetwarzania danych osobowych.
Agencja Wywiadu			Aktualizacja odesłań w ustawie pragmatycznej do przepisów stanowiących samoistną podstawę przetwarzania danych osobowych.
Centralne Biuro Antykorupcyjne			Aktualizacja odesłań w ustawie pragmatycznej do przepisów stanowiących samoistną podstawę przetwarzania danych osobowych.
Służba Kontrwywiadu Wojskowego			Aktualizacja odesłań w ustawie pragmatycznej do przepisów stanowiących samoistną podstawę przetwarzania danych osobowych.
Służba Wywiadu Wojskowego			Aktualizacja odesłań w ustawie pragmatycznej do przepisów stanowiących samoistną podstawę przetwarzania danych osobowych.
Inspekcja Transportu Drogowego			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie

			nowych obowiązków względem osób, których dane dotyczą.
Państwowa Straż Rybacka			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Społeczna Straż Rybacka			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Dyrektor urzędu morskiego, dyrektor urzędu żeglugi śródlądowej.			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Straż Ochrony Kolei			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Inspekcja Ochrony Środowiska			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Straż Leśna			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym

			celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Państwowa Straż łowiecka			Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.
Obywatele	38,4 mln	Główny Urząd Statystyczny. STAN I STRUKTURA LUDNOŚCI; Ludność; 2017; Tablice bilansowe – Stan, ruch naturalny oraz migracje ludności;	Określenie nowych ram prawnych przetwarzania danych osobowych, w tym celów, zakresu przedmiotowego i podmiotowego oraz nadzoru, a także nałożenie nowych obowiązków względem osób, których dane dotyczą.

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

Przygotowanie projektu poprzedził cykl spotkań, w których uczestniczyli przedstawiciele Prokuratury Krajowej, Ministerstwa Sprawiedliwości, Ministerstwa Finansów, Kolegium ds. Służb Specjalnych, Centralnego Biura Antykorupcyjnego, Agencji Bezpieczeństwa Wewnętrznego oraz innych służb specjalnych, a także Policji, Straży Granicznej, Służby Ochrony Państwa, Żandarmerii Wojskowej, Służby Więziennej. W efekcie wypracowano propozycje rozwiązań odnoszących się zarówno do zakresu podmiotowego i przedmiotowego regulacji, jak również szczegółowych zapisów, które stały się podstawą proponowanych w projekcie unormowań. Ministerstwo Spraw Wewnętrznych i Administracji pozostawało również w bezpośrednim kontakcie z Ministerstwem Cyfryzacji w celu zapewnienia spójności przygotowywanych przepisów względem procedowanego w tym czasie projektu ustawy o ochronie danych osobowych, a stanowiącej podstawę wdrożenia w Polsce rozporządzenia UE 2016/679.

Projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Spraw Wewnętrznych i Administracji, stosownie do wymogów art. 5 ustawy z 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz art. 52 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn. zm.) projekt został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji.

Projektowane przepisy poddane zostaną konsultacjom społecznym poprzez skierowanie do:

– Sądu Najwyższego,

– Prokuratora Generalnego,

– Generalnego Inspektora Ochrony Danych Osobowych,

– Szefa Kancelarii Sejmu Rzeczypospolitej Polskiej,

– Szefa Kancelarii Senatu Rzeczypospolitej Polskiej.

Projekt został również przekazany do skonsultowania z Niezależnym Samorządnym Związkiem Zawodowym Pracowników Policji, Niezależnym Samorządnym Związkiem Policjantów i Związkiem Zawodowym Pracowników Ministerstwa Spraw Wewnętrznych i Administracji Publicznej w związku z projektowaną zmianą ustawy o Policji, wprowadzającą podstawę prawną do pobierania od funkcjonariuszy i pracowników Policji odcisków linii papilarnych lub wymazów ze śluzówki policzków w celach eliminacyjnych.

W kontekście uwag zgłaszanych w zakresie zgodności projektowanych rozwiązań z prawem Unii Europejskiej zorganizowano cykl spotkać z udziałem przedstawicieli Ministerstwa Spraw Zagranicznych, Ministerstwa

Sprawiedliwości, Prokuratury Krajowej, Ministerstwa Cyfryzacji, Rządowego Centrum Legislacji oraz Koordynatora ds. Służb Specjalnych.

W projekcie uwzględniono również liczne spośród uwag zgłaszanych przez Prezesa Urzędu Ochrony Danych Osobowych czy Radę Legislacyjną.

6. Wpływ na sektor finansów publicznych[1)]

(ceny stałe z … r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	**0,09**	**0,36**	**0,39**	**0,39**	**0,39**	**0,39**	**0,39**	**0,39**	**0,39**	**0,39**	**0,39**	**3,96**
budżet państwa – udział w podatku PIT (zwielokrotniona przez wskaźnik CPI)	0,01	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,51
JST – udział w podatku PIT (zwielokrotniona przez wskaźnik CPI)	0,01	0,05	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,6
pozostałe jednostki (oddzielnie)												
NFZ (suma składek od pensji nowozatrudnionych pracowników UODO zwielokrotniona przez wskaźnik CPI)	0,03	0,1	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11	1,12
FUS i FP (zwielokrotnione o wskaźnik CPI)	0,04	0,16	0,17	0,17	0,17	0,17	0,17	0,17	0,17	0,17	0,17	1,73
Wydatki ogółem	**0,31**	**1,25**	**1,35**	**1,38**	**1,41**	**1,45**	**1,49**	**1,53**	**1,57**	**1,61**	**1,65**	**15**
budżet państwa	0,3 KP **0,31 KC PI**	1,19 KP **1,25 KC PI**	1,26 KP **1,35 KC PI**	1,26 KP **1,38 KC PI**	1,26 KP **1,41 KC PI**	1,26 KP **1,45 KC PI**	1,26 KP **1,49 KC PI**	1,26 KP **1,53 KC PI**	1,26 KP **1,57 KC PI**	1,26 KP **1,61 KC PI**	1,26 KP **1,65 KC PI**	**15**
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	**(-) 0,22**	**(-) 0,89**	**(-) 0,96**	**(-) 0,99**	**(-) 1,02**	**(-) 1,06**	**(-) 1,1**	**(-) 1,14**	**(-) 1,18**	**(-) 1,22**	**(-) 1,26**	**(-) 11,04**
budżet państwa – wszystkie wydatki	**(-) 0,31**	**(-) 1,25**	**(-) 1,35**	**(-) 1,38**	**(-) 1,41**	**(-) 1,45**	**(-) 1,49**	**(-) 1,53**	**(-) 1,57**	**(-) 1,61**	**(-) 1,65**	**(-) 15**
budżet państwa – dochody z podatku PIT	0,01	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,51
JST – dochody z podatku PIT	0,01	0,05	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,6

[1)] Kwoty podane w ww. tabeli zostały zaokrąglone, zgodnie z ogólnymi zasadami, do wielokrotności liczby 1000000 zł.

pozostałe jednostki (oddzielnie)												
NFZ	0,03	0,1	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11	1,12
FUS oraz FP	0,04	0,16	0,17	0,17	0,17	0,17	0,17	0,17	0,17	0,17	0,17	1,73

Źródła finansowania	Wyjaśnienia do tabeli: KP – kwota podstawowa obejmująca w poszczególnych latach wydatki płacowe KCPI – KP zwielokrotniona o wskaźnik CPI Wydatki budżetu państwa (część 27-Informatyzacja, budżet Polskiego Centrum Akredytacji) będą ponoszone bez konieczności dodatkowego zwiększania limitów. Wydatki w części 10 – Prezes Urzędu Ochrony Danych Osobowych zostaną zwiększone w 2018 r. zgodnie ze wskazanymi powyżej limitami. Wskazać należy, że skutki finansowe wejścia w życie ustawy w 2018 r., wynoszące 295.830 zł, całkowicie zmieszczą się w limicie 650.000 zł, to jest w limicie, o jaki został zwiększony w 2018 r. budżet Generalnego Inspektora Ochrony Danych Osobowych/Prezesa Urzędu Ochrony Danych Osobowych. **W 2018 r. nie zaistnieje potrzeba zwiększania tego limitu.** **W następnych latach limit ten będzie zwiększany w ustawach budżetowych na kolejne lata, zgodnie z prognozą zawartą w niniejszej ocenie skutków regulacji.** Pozostałe podmioty, na które oddziałuje projekt – wydatki związane z projektem ustawy konieczne do poniesienia przez dysponentów środków budżetu państwa, których dotyczą jej przepisy zostaną sfinansowane w ramach limitów wydatków planowanych we właściwych dla dysponentów częściach budżetu państwa na dany rok, bez konieczności ich zwiększania, a wejście w życie projektowanych przepisów nie będzie stanowiło podstawy do ubiegania się o dodatkowe środki z budżetu państwa na ten cel.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nowo utworzona struktura włączona do Urzędu Ochrony Danych Osobowych zatrudniać będzie **15 pracowników cywilnych – pracowników urzędów państwowych w rozumieniu ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. z 2017 r., poz. 2142 – tekst jednolity, z późn. zm.). Art. 1 ust. 1 pkt 13 wymienionej ustawy wskazuje, że ustawa ta określa obowiązki i prawa urzędników państwowych oraz innych pracowników zatrudnionych m.in. w Urzędzie Ochrony Danych Osobowych.** Pracownicy Urzędu Ochrony Danych osobowych nie są objęci mnożnikowym systemem ustalania wynagrodzeń, a ponadto budżet UODO nie podlega weryfikacji przez Ministra Finansów na etapie tworzenia ustawy budżetowej, co wynika z art. 139 ust. 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r., poz. 2077 – tekst jednolity, z późn. zm.). Za podstawę kalkulacji wydatków związanych z zatrudnieniem w Urzędzie Ochrony Danych Osobowych nowych 15 pracowników przyjęto zatem obowiązującą w UODO kwotę średniego wynagrodzenia pracowników tego urzędu. Z informacji uzyskanych na roboczo od Głównego Księgowego w Urzędzie Ochrony Danych Osobowych, średnie wynagrodzenie pracowników Urzędu Ochrony Danych Osobowych (dawnego Biura Generalnego Inspektora Ochrony Danych Osobowych) za 2017 r., wyliczone według sprawozdania Rb 70, łącznie z dodatkowym wynagrodzeniem rocznym (tzw. „trzynastką") wynosi **6960 zł**, natomiast bez dodatkowego wynagrodzenia rocznego wynosi **6574 zł**. Średnia wysokość dodatkowego wynagrodzenia rocznego stanowi różnicę pomiędzy wskazanymi kwotami, zwielokrotnioną przez 12 miesięcy i wynosi 386 zł x 12 miesięcy = **4.632 zł**. Przyjęto założenie, że ustawa wejdzie w życie przed dniem 1 października 2018 r. i od tej daty będzie możliwe rozpoczęcie rekrutacji nowych pracowników. Mając powyższe na uwadze, koszt płac 15 nowo zatrudnionych pracowników UODO będzie się kształtować następująco: **dla 2018 r (październik – grudzień),** **15 pracowników cywilnych x 6574 zł średniego wynagrodzenia (bez dodatkowego wynagrodzenia rocznego) x 3 miesiące = 295.830 zł.**

	dla 2019 r. **15 pracowników cywilnych x 6574 zł średniego wynagrodzenia (bez dodatkowego wynagrodzenia rocznego) x 12 miesiące = 1.183.320 zł.** Uwaga: Nowo zatrudnieni pracownicy nie otrzymają w 2019 r. dodatkowego wynagrodzenia rocznego, ponieważ warunkiem nabycia uprawnienia do takiego wynagrodzenia jest przepracowanie przynajmniej 6 miesięcy u danego pracodawcy. **dla lat 2020–2028** **15 pracowników cywilnych x 6960 zł średniego wynagrodzenia (wraz z dodatkowym wynagrodzeniem rocznym) x 12 miesiące = 1.252.800 zł.** Niezależnie od ponoszonych kosztów przez budżet państwa w związku z koniecznością ponoszenia nakładów na płace dodatkowych pracowników zatrudnionych w UODO, wskazać należy, że płace te będą podlegały opodatkowaniu podatkiem PIT oraz od płac pracowników będą odprowadzane składki do Narodowego Funduszu Zdrowia oraz Funduszu Ubezpieczeń Społecznych. Kalkulacja rocznych dochodów z podatku PIT przedstawia się następująco: Fundusz wynagrodzeń powiększony o dodatkowe wynagrodzenie roczne (z wyjątkiem okresu październik–grudzień 2018 r. oraz całego 2019 r.), pomniejszony o składki odprowadzane na Fundusz Ubezpieczeń Społecznych (13,71%) stanowi podstawę opodatkowania podatkiem PIT w wysokości 18% oraz podstawę do wyliczenia części składek zdrowotnych w wysokości 7,75%. Różnica pomiędzy obliczonym podatkiem PIT oraz kwotą składek zdrowotnych będzie stanowić kwotę rzeczywistego dochodu z podatku od dochodów osób fizycznych, który będzie podlegać podziałowi pomiędzy jednostki samorządu terytorialnego oraz budżet państwa. W roku 2018 (październik – grudzień) **Fundusz płac w wysokości 295.830 zł pomniejszony o składki na ubezpieczenia społeczne (295.830 zł x 13,71% = 40.558 zł 30 gr) = 255.271 zł 70 gr podstawy opodatkowania.** 255.271 zł 70 gr x 18% podatku PIT = 45.948 zł 90 gr 255.271 zł 70 gr x 7.75% składki zdrowotnej = 19.783 zł 56 gr Dochód z podatku PIT wyniesie zatem 45.948 zł 90 gr – 19.783 zł 56 gr = **26.165 zł 34 gr** z czego **do budżetów jednostek samorządu terytorialnego trafi** łącznie 51,19% tej kwoty (zgodnie z przepisami ustawy z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego – Dz. U. z 2018 r., poz. 1530, z późn. zm.), to jest **13.394 zł 03 gr**, natomiast **do budżetu państwa trafi 12.771 zł 31 gr.** W roku 2019 **Fundusz płac w wysokości 1.183.320 zł pomniejszony o składki na ubezpieczenia społeczne (1.183.320 zł x 13,71% = 162.233 zł 17 gr) = 1.021.086 zł 83 gr podstawy opodatkowania.** 1.021.086 zł 83 gr 18% podatku PIT = 183.795 zł 63 gr 1.021.086 zł 83 gr x 7.75% składki zdrowotnej = 79.134 zł 23 gr Dochód z podatku PIT wyniesie zatem 183.795 zł 63 gr – 79.134 zł 23 gr = **104.661 zł 40 gr** z czego **do budżetów jednostek samorządu terytorialnego trafi** łącznie 51,19% tej kwoty (zgodnie z przepisami ustawy z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego), to jest **53.576 zł 17 gr**, natomiast **do budżetu państwa trafi 51.085 zł 23 gr.** W latach 2020–2028. **Fundusz płac w wysokości 1.252.800 zł pomniejszony o składki na ubezpieczenia społeczne (1.252.800 zł x 13,71% = 171.758 zł 88 gr) = 1.081.041 zł 12 gr podstawy opodatkowania.** 1.081.041 zł 12 gr x 18% podatku PIT = 194.587 zł 40 gr 1.081.041 zł 12 gr x 7.75% składki zdrowotnej = 83.780 zł 70 gr Dochód z podatku PIT wyniesie zatem 194.587 zł 40 gr – 83.780 zł 70 gr = **110.806 zł 70 gr** z czego **do budżetów jednostek samorządu terytorialnego trafi** łącznie 51,19% tej kwoty (zgodnie z przepisami ustawy z dnia 13 listopada 2003 r. o dochodach jednostek samorządu

terytorialnego) to jest **56.721 zł 95 gr**, natomiast **do budżetu państwa trafi 54.084 zł 75 gr.**

Nowo zatrudnieni pracownicy UODO będą odprowadzać składki do Narodowego Funduszu Zdrowia, zatem roczny dochód NFZ będzie kształtować się następująco:

W roku 2018

295.830 zł kwoty przeznaczonej na roczne płace nowozatrudnionych pracowników UODO x 9% wymiaru składki wynikającego z art. 79 ust.1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2018 r. poz. 1510, z późn. zm.) = **26.624 zł 70 gr.**

W roku 2019

1.183.320 zł kwoty przeznaczonej na roczne płace nowo zatrudnionych pracowników UODO x 9% wymiaru składki wynikającego z art. 79 ust.1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych = **106.498 zł 80 gr.**

W latach 2020–2028

1.252.800 zł kwoty przeznaczonej na roczne płace nowo zatrudnionych pracowników UODO x 9% wymiaru składki wynikającego z art. 79 ust.1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych = **112.752 zł.**

Nowo zatrudnieni pracownicy UODO będą także odprowadzać składki do Funduszu Ubezpieczeń Społecznych. Jak to zostało wykazane powyżej, suma składek pracowników cywilnych odprowadzanych do FUS oraz FP wyniesie:

w 2018 r. – **40.558 zł 30 gr,**

w 2019 r. – **162.233 zł 17 gr**,

w latach 2020–2028 – **171.758 zł 88 gr.**

Wykazane powyżej koszty płacowe zostały zwaloryzowane o wskaźnik „CPI-dynamika średnioroczna" zawarty w zatwierdzonych 25 maja 20187 r. przez Ministra Finansów „Wytycznych dotyczących stosowania jednolitych wskaźników makroekonomicznych będących podstawą oszacowania skutków finansowych projektowanych ustaw".

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 wejście w życie nowej ustawy spowoduje wzrost zatrudnienia w UODO, a co za tym idzie 15 osób zacznie otrzymywać wynagrodzenie	295.830 zł (rocznie brutto) – 13.71% udziału pracownika w składce do FUS – 18% podatku dochodowego od osób fizycznych – 1,5% udziału pracownika	1.183.320 zł (rocznie brutto) – 13.71% udziału pracownika w składce do FUS – 18% podatku dochodowego od osób fizycznych – 1,5% udziału	1.252.800 zł (rocznie brutto) – 13.71% udziału pracownika w składce do FUS – 18% podatku dochodowego od osób fizycznych – 1,5% udziału	1.252.800 zł (rocznie brutto) – 13.71% udziału pracownika w składce do FUS – 18% podatku dochodowego od osób fizycznych – 1,5% udziału	1.252.800 zł (rocznie brutto) – 13.71% udziału pracownika w składce do FUS – 18% podatku dochodowego od osób fizycznych – 1,5% udziału	1.252.800 zł (rocznie brutto) – 13.71% udziału pracownika w składce do FUS – 18% podatku dochodowego od osób fizycznych – 1,5% udziału	Łącznie średni dochód netto jednego pracownika w okresie 10 lat oraz 3 ostatnich miesięcy 2018 r. wyniesie: (3 x 4.566 zł 50 gr) + (12 x 4.566 zł 50 gr) + [9 x (12 x 4.834 zł 65 gr)] =

	za płacę	w składce do NFZ = 255.271 zł 70 gr (po potrąceniach na FUS) – 45.948 zł 90 gr (podatku PIT) – 3.829 zł 10 gr (udział pracownika w składce na NFZ) = **205.493 zł 70 gr dochodu netto** 205.493 zł 70 gr/15 pracowników /3 miesiące = **4.566 zł 50 gr miesięcznego dochodu netto na jednego pracownika.**	pracownika w składce do NFZ = 1.021.086 zł 80 gr (po potrąceniach na FUS) – 183.795 zł 60 gr (podatku PIT) – 15.316 zł 30 gr (udział pracownika w składce na NFZ) = **821.974 zł 90 gr dochodu netto** 821.974zł 90 gr/15 pracowników /12 miesięcy = **4.566 zł 50 gr miesięcznego dochodu netto na jednego pracownika.**	pracownika w składce do NFZ = 1.081.041 zł 10 gr (po potrąceniach na FUS) – 194.587 zł 40 gr (podatku PIT) – 16.215 zł 60 gr (udział pracownika w składce na NFZ) = **870.238 zł 10 gr dochodu netto** 870.238zł 10 gr/15 pracowników /12 miesięcy = **4.834 zł 65 gr miesięcznego dochodu netto na jednego pracownika.**	pracownika w składce do NFZ = 1.081.041 zł 10 gr (po potrąceniach na FUS) – 194.587 zł 40 gr (podatku PIT) – 16.215 zł 60 gr (udział pracownika w składce na NFZ) = **870.238 zł 10 gr dochodu netto** 870.238zł 10 gr/15 pracowników /12 miesięcy = **4.834 zł 65 gr miesięcznego dochodu netto na jednego pracownika.**	pracownika w składce do NFZ = 1.081.041 zł 10 gr (po potrąceniach na FUS) – 194.587 zł 40 gr (podatku PIT) – 16.215 zł 60 gr (udział pracownika w składce na NFZ) = **870.238 zł 10 gr dochodu netto** 870.238zł 10 gr/15 pracowników /12 miesięcy = **4.834 zł 65 gr miesięcznego dochodu netto na jednego pracownika.**	pracownika w składce do NFZ = 1.081.041 zł 10 gr (po potrąceniach na FUS) – 194.587 zł 40 gr (podatku PIT) – 16.215 zł 60 gr (udział pracownika w składce na NFZ) = **870.238 zł 10 gr dochodu netto** 870.238zł 10 gr/15 pracowników /12 miesięcy = **4.834 zł 65 gr miesięcznego dochodu netto na jednego pracownika.**	13.699 zł 50 gr + 54.798 zł + 522.142 zł 20 gr = **590.639 zł 70 gr**
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
Niemierzalne								
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projekt nie będzie miał wpływu na konkurencyjność gospodarki i przedsiębiorczość. Natomiast jego celem jest skuteczniejsza ochrona danych osobowych osób, których dane są przetwarzane przez uprawnione do tego osoby, tym samym oddziaływać będzie na obywateli, wprowadzając stosowne instrumenty gwarancyjne w odniesieniu do wartości konstytucyjnych objętych zakresem regulacji. Projektowane przepisy poszerzają obowiązek informacyjny wobec osób, których dane osobowe będą przetwarzane, uwzględniając transparentność przetwarzania danych. Projektowana ustawa nie będzie miała wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych.							

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:

Projekt ustawy nakłada na podmioty przetwarzające dane osobowe dodatkowe obowiązki informacyjne wobec osób, których dane dotyczą.

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.

Projekt ustawy znosi ogólny obowiązek dokumentacyjny w zakresie ochrony danych osobowych. Został on zastąpiony zasadą rozliczalności.

Jednak wprowadzenie dodatkowych instrumentów gwarancyjnych służących ochronie danych osobowych przetwarzanych w związku z celami określonymi w ustawie skutkować będzie zwiększeniem liczby wewnętrznych procedur oddziałujących na podmioty przetwarzające dane osobowe, a także wiązać się może z przeprowadzeniem audytów systemów i procesów przetwarzania danych.

Podmioty przetwarzające, dla których przetwarzanie danych osobowych uprzednio nie było głównym przedmiotem działania, przynajmniej początkowo, odczują obowiązek dostosowania się do przyjętych w ustawie rozwiązań, głównie z uwagi na wzrost ilości informacji, które trzeba będzie przekazać osobom, których dane te dotyczą.

9. Wpływ na rynek pracy

Projekt przepisów ustawy o ochronie danych osobowych będzie pozytywnie wpływał na rynek pracy, jednak oddziaływanie to nie będzie znaczące. Na zwiększenie liczby miejsc pracy wpłynie zwiększenie liczby etatów w Urzędzie Ochrony Danych Osobowych.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne

☐ sytuacja i rozwój regionalny

☒ inne: Wolności i prawa obywateli

Omówienie wpływu	W wyniku wejścia w życie projektowanych przepisów niezbędne będzie dostosowanie systemów teleinformatycznych do nowych przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

11. Planowane wykonanie przepisów aktu prawnego

Zgodnie z art. 63 ust. 1 dyrektywy 2016/680, państwa członkowskie do dnia 6 maja 2018 r. mają obowiązek przyjęcia i opublikowania przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do wykonania dyrektywy. Ustawa wchodzi w życie 14 dni od dnia ogłoszenia.

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

Po upływie dwóch lat od wejścia w życie projektowanych przepisów planuje się wystąpienie do podmiotów funkcjonujących w sferze wyznaczonej przez zakres przedmiotowy dyrektywy 2016/680, w celu przedstawienia opinii na temat funkcjonowania przyjętych w ustawie rozwiązań. W ramach analizy pod uwagę zostanie wzięta zarówno ocena skuteczności wprowadzanych instrumentów prawnych w zakresie ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jak i ich adekwatność względem celów wynikających z dyrektywy 2016/680.

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

Brak załącznika.

W ramach konsultacji publicznych projekt ustawy *o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* został skierowany do:

- Niezależnego Samorządnego Związku Zawodowego Policjantów (19 kwietnia 2018 r.),

- Niezależnego Samorządnego Związku Zawodowego Pracowników Policji (19 kwietnia 2018 r.),

- Związku Zawodowego Pracowników Ministerstwa Spraw Wewnętrznych i Administracji Publicznej (19 kwietnia 2018 r.),

- Niezależnego Samorządnego Związku Zawodowego „Solidarność" (20 kwietnia 2018 r.),

- Forum Związków Zawodowych (20 kwietnia 2018 r.),

- Ogólnopolskiego Porozumienia Związków Zawodowych (20 kwietnia 2018 r.),

- Krajowej Rady Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej (19 kwietnia 2018 r.),

- do następujących fundacji: Helsińskiej Fundacji Praw Człowieka, Amnesty International, Fundacji im. Stefana Batorego, Fundacji Panoptykon, Sieci Obywatelskiej Watchdog Polska (20 kwietnia 2018 r.),

- Pracodawców Rzeczypospolitej Polskiej, Konfederacji Lewiatan, Business Centre Club - Związku Pracodawców, Polskiego Związku Pracodawców Ochrona (20 kwietnia 2018 r.).

Uwagi do projektu zgłosiła Fundacja Panoptykon pismem z dnia 4 maja 2018 r.

Warszawa, 5 października 2018 r.

[redacted]

Minister
Spraw Zagranicznych

DPUE.920.582.2018/54/JS,mp

dot.: RM-10-124-18 z 3.10.2018 r. (Tekst ostateczny)

Pan
Jacek Sasin
Sekretarz Rady Ministrów

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

Szanowny Panie Ministrze,

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

1. **Wyłączenie dotyczące akt sprawy**

Zgodnie z **art. 3 pkt 1 projektu ustawy** przepisów tej ustawy nie stosuje się do ochrony danych osobowych znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie wskazanych ustaw, w tym np. na podstawie Kodeksu postępowania karnego.

Projektowane wyłączenie dotyczy zatem akt sprawy przechowywanych zarówno w wersji papierowej, jak i danych osobowych przetwarzanych z wykorzystaniem technik informatycznych.

Zgodnie z art. 2 ust. 2 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 jej przepisy mają 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.

Z kolei art. 3 pkt 6 dyrektywy 2016/680/UE wskazuje, że zbiór danych oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie. Przepis

ten wymaga jedynie, by zbiór był uporządkowanym zestawem danych osobowych dostępnych według określonych kryteriów.

Po pierwsze należy zauważyć, że z przepisu tego nie wynika, że kryteria te muszą mieć charakter osobowy, jak wskazuje w uzasadnieniu projektodawca. Należy podkreślić, że Trybunał Sprawiedliwości UE zinterpretował pojęcie zbioru danych w wyroku z dnia 10 lipca 2018 r. w sprawie C-25/17. Sprawa ta dotyczyła pojęcia zbioru danych obowiązującego na gruncie uchylonej już dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Chociaż dyrektywa ta nie obejmowała działalności państwa członkowskiego w obszarach prawa karnego, to jednak należy uznać, że tezy tego wyroku powinny być pewną wskazówką interpretacyjną również na gruncie dyrektywy 2016/680/UE, w której definicja zbioru danych jest tożsama.

We wskazanej sprawie dane osobowe były zbierane w ramach działalności kaznodziejskiej realizowanej poprzez odwiedzanie kolejnych gospodarstw domowych i robienie zapisków ku pamięci, na podstawie podziału według obszarów geograficznych, po to, aby ułatwić organizowanie późniejszych wizyt składanych u osób, które zostały już odwiedzone. Dane te były zorganizowane według kryteriów przyjętych w zależności od celu, któremu miało służyć ich gromadzenie, tj. przygotowywanie kolejnych wizyt. Trybunał Sprawiedliwości uznał, że pojęcie „zbioru danych" może obejmować zestaw danych osobowych gromadzonych w ramach działalności kaznodziejskiej realizowanej przez odwiedzanie kolejnych gospodarstw domowych, a ponadto stwierdził, że aby taki zestaw był objęty pojęciem zbioru danych, nie jest konieczne, by zawierał kartoteki, szczególne rejestry lub inne systemy służące wyszukiwaniu.

Należy zatem uznać, że kryterium podziału nie musi odnosić się do kwestii osobowych, nie musi tym samym istnieć możliwość wyszukiwania w zbiorze danych osobowych poprzez wskazanie imienia, nazwiska lub nr PESEL.

Po drugie należy wskazać, że chociaż w definicji zbioru danych, która znalazła się w dyrektywie policyjnej użyto sformułowania „kryteria" w liczbie mnogiej, w sprawie C-25/17 Trybunał Sprawiedliwości wskazał, że wystarczającym kryterium jest podział geograficzny (a zatem, że wystarczy jedno kryterium). Trybunał Sprawiedliwości podkreślił również, że dla uznania, że dane osobowe są lub że mogą być zgromadzone w zbiorze danych nie ma znaczenia kwestia według jakiego konkretnego kryterium i w jakiej dokładnie postaci zestaw danych osobowych jest faktycznie zorganizowany. Nie można podzielić zatem również tego argumentu projektodawcy.

Niezależnie od powyższego należy wskazać, że do uznania, że akta sprawy mieszczą się w pojęciu zbioru danych wystarczy, że dane osobowe zawarte w tych aktach są uporządkowane np. według numeru sprawy, czy rodzaju sprawy, a następnie w aktach konkretnej sprawy, aby były uporządkowane np. chronologicznie. Kryterium może być też np. wskazanie, że dana sprawa jest prowadzona przeciwko konkretnemu oskarżonemu. W tym przypadku można wyróżnić co najmniej kilka kryteriów w rozumieniu art. 3 pkt 6 dyrektywy 2016/680/UE.

Ponadto należy zauważyć, że zgodnie z uzasadnieniem do projektu ustawy zestaw danych, podlegający definicji zawartej w prawie unijnym, musi zdaniem projektodawcy posiadać strukturę, rozumianą jako jednorodna budowa zbioru.

Należy jednak wskazać, że w ww. wyżej wyroku w sprawie C-25/17 Trybunał Sprawiedliwości uznał, że prowadzone w ramach działalności kaznodziejskiej zapiski są objęte pojęciem zbioru danych, pomimo, że nie zawierają kartotek, szczególnych rejestrów lub innych systemów służących wyszukiwaniu danych osobowych. Również w tym aspekcie nie można zatem zgodzić się z projektowanym wyłączeniem.

Niemniej istotne jest także to, że zaproponowane przez projektodawcę rozwiązanie stałoby w sprzeczności z celowościową wykładnią przepisów dyrektywy 2016/680/UE. Wyłączenie spod zakresu zastosowania ustawy wdrażającej tę dyrektywę akt postępowania, w których znajduje się znacząca ilość danych osobowych, godzi w cel dyrektywy, którym jest ustanowienie przepisów o ochronie danych osobowych przetwarzanych w celu zwalczania przestępczości. Można bowiem przyjąć, że przy zastosowaniu wyłączenia poza zakresem dyrektywy 2016/680/UE znalazłaby się większość danych osobowych, skoro postępowanie karne jest prowadzone w oparciu o akta sprawy.

Należy zatem uznać, że projektowany art. 3 pkt 1 jest sprzeczny z art. 2 ust. 2 w zw. z art. 3 pkt 6 dyrektywy 2016/680/UE.

Jednocześnie należy zauważyć, że w odniesieniu do danych przetwarzanych w sposób choćby częściowo automatyczny, przepisy dyrektywy 2016/680/UE mają zastosowanie niezależnie od tego, czy dane osobowe stanowią lub mają stanowić część zbioru danych – wskazuje na to wprost art. 2 ust. 2 ww. dyrektywy. Projektowane wyłączenie dotyczące danych osobowych przetwarzanych z wykorzystaniem technik informatycznych jest zatem sprzeczne z art. 2 ust. 2 dyrektywy 2016/680/UE.

2. **Wyłączenie w zakresie bezpieczeństwa narodowego**

Zgodnie z **art. 3 pkt 2 projektu ustawy** nie stosuje się jej przepisów do danych osobowych przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego. Sformułowanie „w tym w ramach realizacji zadań ustawowych ABW, AW, SKW, SWW oraz CBA" wskazuje na podmiotowe wyłączenie stosowania ustawy do działalności ustawowej tych służb.

Tymczasem zgodnie z art. 2 ust. 3 lit. a dyrektywy 2016/680/UE, ten akt prawny nie ma zastosowania do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa Unii Europejskiej. W ocenie MSZ przepis ten nie pozwala na podmiotowe wyłączenie służb specjalnych. Przepis ten wskazuje jedynie, że dyrektywy 2016/680/UE nie stosuje się do działalności pozostającej poza zakresem prawa unijnego. Wyłączenie służb musi mieć zatem charakter przedmiotowy (działalność w zakresie bezpieczeństwa narodowego), a nie podmiotowy (cała działalność służb).

Wszystkie regulacje unijne (np. 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 - ogólne rozporządzenie o ochronie danych, tzw. RODO) wskazujące, że bezpieczeństwo narodowe jest dziedziną nieobjętą prawem UE odwołują się do prowadzenia działalności, wykonywania czynności i pełnienia funkcji mających na celu ochronę bezpieczeństwa narodowego. Poza regulacją unijną jest bowiem sama działalność prowadzona w celu ochrony bezpieczeństwa narodowego, a nie podmiot prowadzący tę działalność jako taki.

Również motyw 14 preambuły do dyrektywy 2016/680/UE potwierdza takie stanowisko. Wskazuje on bowiem ogólnie, że poza zakresem dyrektywy pozostaje „działalność wykraczającą poza zakres prawa Unii", natomiast pozostałe jego elementy, tj. „czynności w zakresie bezpieczeństwa narodowego" i „czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym" są jedynie dopełnieniem pierwszego wyrażenia i stanowią jego przykład - świadczy o tym zarówno brzmienie art. 2 ust. 3 lit. a dyrektywy 2016/680/UE, jak i

użycie słowa „dlatego" po wyrażeniu „niniejsza dyrektywa nie powinna mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii".

Ponadto przypominam, że kwestia możliwości podmiotowego wyłączenia służb specjalnych została skonsultowana z Komisją Europejską. Komisja przedstawiła swoje stanowisko, zgodnie z którym tego typu wyłączenie jest niezgodne z prawem unijnym. Miało to miejsce w związku z pracami związanymi z RODO, jednak zarówno RODO, jak i dyrektywa 2016/680/UE posługują się tym samym sformułowaniem odnoszącym się do działalności nieobjętej prawem UE. Można zatem uznać, że stanowisko to będzie aktualne również na gruncie ww. dyrektywy.

Powyższe rozważania znajdują potwierdzenie również w prawie krajowym. Nie wszystkie działania ustawowe ww. służb (projektowane wyłączenie będzie natomiast stosowane do wszystkich działań) mieszczą się bowiem w zakresie pojęcia bezpieczeństwa narodowego – szczególnie wątpliwe jest wyłączenie CBA, ponieważ jest to służba powołana do zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, w tym do rozpoznawania, zapobiegania i wykrywania przestępstw w tym zakresie (art. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym). Do takiej działalności powinny być stosowane przepisy dyrektywy 2016/680/UE.

Uwzględniając powyższe proponuję przeformułować art. 3 pkt 2 projektu ustawy.

Projekt ustawy jest zgodny z prawem Unii Europejskiej z zastrzeżeniem powyższych uwag.

Z poważaniem

z up. Ministra Spraw Zagranicznych
Bartosz Cichocki
Podsekretarz Stanu

Do wiadomości:
Pan Joachim Brudziński
Minister Spraw Wewnętrznych i Administracji