

**Dz.U. 2019 poz. 125****USTAWA**

z dnia 14 grudnia 2018 r.

**o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości<sup>1), 2)</sup>**

## Rozdział 1

**Przepisy ogólne****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;

<sup>1)</sup> 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 uchyłającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89).

<sup>2)</sup> 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 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.

- 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 urzędzeniach 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, 1387 i 2432), ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2018 r. poz. 1987 i 2399), ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2018 r. poz. 1958, 2192, 2193, 2227 i 2354), ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475, z późn. zm.<sup>3)</sup>), 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, z 2016 r. poz. 2205 oraz z 2018 r. poz. 2435), 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);
- 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 Unii Europejskiej 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.<sup>4)</sup>);
- 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 władzy 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 Unii Europejskiej, a przetwarzanie tych danych jest zgodne z przepisami o ochronie danych mającymi zastosowanie do ich celów przetwarzania;

<sup>3)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 1039, 1387, 1467, 1481 i 2077 oraz z 2019 r. poz. 76.

<sup>4)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L127 z 23.05.2018, str. 2.

- 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) państwie trzecim – rozumie się przez to państwo niebędące państwem członkowskim Unii Europejskiej i niestosujące przepisów dorobku Schengen;
- 12) 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;
- 13) 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;
- 14) 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;
- 15) 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;
- 16) właściwym organie – rozumie się przez to organ władzy publicznej, jednostkę organizacyjną lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych;
- 17) 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;
- 3) doradzanie instytucjom publicznym w sprawach środków ochrony praw i wolności osób fizycznych w 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 władzy publicznej;
- 9) pełnienie funkcji konsultacyjnych, o których mowa w art. 38, dotyczących operacji przetwarzania w ramach niniejszej ustawy;
- 10) współpraca z organami nadzorczymi w innych 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 ustaw i rozporządzeń w sprawach dotyczących ochrony danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1.

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. Projekty ustaw i rozporządzeń dotyczące danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1, 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. 2, 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 obowiązany 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 obowiązany 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 9, 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. Administrator lub podmiot przetwarzający, 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 sprawdzenia, 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.** Do postępowań w sprawach objętych zakresem regulacji niniejszego rozdziału stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2018 r. poz. 2096 oraz z 2019 r. poz. 60), 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 uprawnień 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 w innych celach niż określone w art. 1 pkt 1, jeżeli przepisy prawa 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 zezwalają na ich przetwarzanie lub
- 2) jest to niezbędne dla ochrony życia lub zdrowia lub 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 dopuszczają je przepisy prawa, 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 przysyłać 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, przysyłając dane osobowe odbiorcy, o którym mowa w ust. 1, przekazuje, w miarę potrzeby i możliwości, niezbędne dodatkowe informacje pozwalające temu odbiorcy ocenić stopień prawidłowości, kompletności oraz aktualności przesyłanych danych osobowych.

3. Właściwy organ, który przesłał odbiorcy, o którym 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 tego odbiorcę oraz:

- 1) sprostować, uzupełnić lub uaktualnić te dane, a także przesłać temu 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 tego odbiorcę w celu usunięcia lub ograniczenia przez tego 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 odbiorcy, o którym 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 zezwalają szczególne warunki przetwarzania, właściwy organ przysyłający jest obowiązany 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 właściwego organu lub urzędu lub w jego siedzibie.

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 niedostępności tych danych odbiorcom.

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

3. Administrator bez zbędnej zwłoki informuje odbiorców o dokonanych sprostowaniach lub usunięciu danych osobowych, lub ograniczeniu ich przetwarzania. Odbiorcy są obowiązani do uaktualnienia, sprostowania lub usunięcia danych osobowych, lub ograniczenia ich przetwarzania.

4. Przed zniesieniem ograniczenia przetwarzania kwestionowanych danych osobowych 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 niniejszego 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 lub art. 24 ust. 1, jest obowiązany 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 w sposób określony w art. 30 ust. 2.

**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 2019 r. poz. 123) 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 opłatę, pokrywającą 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 państwowej jednostki budżetowej albo samorządowej jednostki budżetowej stanowi odpowiednio dochód budżetu państwa albo jednostki samorządu terytorialnego.

6. Administrator bez zbędnej zwłoki, lecz nie później niż w terminie do 14 dni od dnia złożenia wniosku, o którym mowa w art. 22 ust. 4, art. 23 ust. 1 lub art. 24 ust. 1, powiadomi wnioskodawcę o wysokości opłaty, o której mowa w ust. 4 pkt 1. Udzielenie informacji zgodnie z wnioskiem następuje w terminie do 14 dni od uiszczenia opłaty, 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 osobowych, 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 obowiązane 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 osobowych, 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, 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, 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, o której mowa w ust. 1, sporządza się w formie 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 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, o której mowa w ust. 1, 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, o której mowa w ust. 1.

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 przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
- 7) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazania, 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 przetwarzania 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 lub podmiot przetwarzający 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 posiadaniem 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:

- 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 odpowiednio 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 obowiązane 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 wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby 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 osobowych, 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) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
- 2) 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;
- 3) 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. Administrator, który wyznaczył inspektora, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności, z uwzględnieniem kryteriów, o których mowa w ust. 2.

5. W związku z wykonywaniem obowiązków inspektora w czasie jego nieobecności do osoby go zastępującej stosuje się odpowiednio przepisy dotyczące inspektora.

6. Podmiot, który wyznaczył osobę zastępującą inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w trybie określonym w ust. 10 oraz udostępnia jego dane zgodnie z ust. 11.

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

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

9. Administrator zawiadamia Prezesa Urzędu o wyznaczeniu inspektora ochrony danych w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora ochrony danych. Zawiadomienie sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem zaufanym. Zawiadomienie może zostać dokonane przez pełnomocnika. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej.

10. Administrator zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 9, oraz o odwołaniu inspektora ochrony danych, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

11. Administrator udostępnia dane inspektora ochrony danych, o których mowa w ust. 9, 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) pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących jej praw, o których mowa w rozdziale 4;
- 9) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37, oraz monitorowanie wykonania tych zaleceń;
- 10) 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 organu nadzorczego w innych państwach Unii Europejskiej z wnioskiem o pomoc, w szczególności o udzielenie 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 organu nadzorczego 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 postępowach 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 w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa Urzędu, pisemnie, faxem, elektronicznie lub za pomocą elektronicznej platformy usług administracji publicznej ePUAP.

4. Prezes Urzędu informuje osobę, która wniosła skargę, o postępowach 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 3 miesięcy od dnia wpływu skargi, o postępowach 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 1629 oraz z 2019 r. poz. 11 i 60), 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.<sup>5)</sup>) o interweniencji ubocznym.

<sup>5)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 1467, 1499, 1544, 1629, 1637, 1693, 2385 i 2432 oraz z 2019 r. poz. 60.

## 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.

## Rozdział 9

**Zmiany w przepisach**

**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 2019 r. poz. 52, 55, 60 i 125) 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 lub 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 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 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególnie 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 lub 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 14 grudnia 2018 r. 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.<sup>6)</sup>) wprowadza się następujące zmiany:

- 1) w art. 1 w ust. 2 pkt 8 otrzymuje brzmienie:  
„8) przetwarzanie informacji kryminalnych, w tym danych osobowych;”;
- 2) w art. 5b w ust. 1 po wyrazach „w zakresie zleconym przez Inspektora Nadzoru Wewnętrznego – funkcjonariuszy i pracowników” dodaje się wyraz „Policji;”;
- 3) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125)”;
- 4) 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;”;

<sup>6)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544, 1669, 2077, 2102, 2245 i 2399 oraz z 2019 r. poz. 15, 53 i 81.

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

„7c. Użyte w ust. 1 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, 5a–7, 9 i 10, wzory dokumentów stosowanych w tych sprawach oraz w odniesieniu do ust. 1 pkt 5b również sposób przechowywania, odtwarzania i kopiowania zapisów obrazu i dźwięku, mając na względzie zapewnienie skuteczności działań podejmowanych przez Policję, poszanowanie praw osób, wobec których działania te są podejmowane oraz konieczność właściwego zabezpieczenia utrwalonego obrazu i dźwięku przed utratą, zniekształceniem, a także zapewnienie ochrony praw osób, których wizerunek został utrwalony.”;

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

„Art. 15b. 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. W przypadku czynności operacyjno-rozpoznawczych terminy, o których mowa w zdaniu pierwszym, są liczone od dnia zakończenia realizacji tych czynności.

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.”;

- 6) 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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.<sup>7)</sup>), 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 niejawnny, odbywać się bez zgody i wiedzy, osoby której dane 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;

<sup>7)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

- 2) uzyskanych przez te służby lub organy w wyniku wykonywania czynności operacyjno-rozpoznawczych, w tym prowadzonej kontroli operacyjnej.

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 14 grudnia 2018 r. 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 słuzówki 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 słuzówki 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 słuzówki 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 słuzówki 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 obowiązane 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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;

7) 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.”;

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

a) w ust. 1 we wprowadzeniu do wyliczenia 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 (Stoleczny) 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 wykrywania przestępstw oraz ścigania ich sprawców, ratowania życia lub zdrowia ludzkiego albo poszukiwania osób zaginionych.”;

9) w art. 20cb:

a) w ust. 1 we wprowadzeniu do wyliczenia 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.”;

10) 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”;

11) 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).”;

12) w art. 20f w ust. 4 wyrazy „ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138, 723 i 1000)” zastępuje się wyrazami „ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości”;

13) dodaje się art. 20g w brzmieniu:

„Art. 20g. 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.”;

14) 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 14 grudnia 2018 r. 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, z 2016 r. poz. 2205 oraz z 2018 r. poz. 2435),
  - 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 nieznanymi 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. 11;
- 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. 11, 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 14 grudnia 2018 r. 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. 11.

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.”;

15) uchyla się art. 21f i art. 21g;

16) 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 „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. 11;
- 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 identyfikacyjnych.

2. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. a–f, 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. 11.

Art. 21l. 1. W weryfikacji, o której mowa w art. 16 ustawy z dnia 14 grudnia 2018 r. 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.”;

- 17) 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.”;

- 18) 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 rozporządzenia (UE) 2016/679, w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie policjantów lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowiązaniu policjantów lub 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.”;

19) 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.<sup>8)</sup>) 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 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. 3c w ust. 1 po wyrazach „w zakresie zleconym przez Inspektora Nadzoru Wewnętrzny – funkcjonariuszy i pracowników Policji” dodaje się wyrazy „, , Straży Granicznej.”;

3) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125)”;

<sup>8)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 106, 138, 650, 730, 894, 1544 i 2399 oraz z 2019 r. poz. 53.

4) 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 umożliwiającą 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.”;

5) 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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.<sup>9)</sup>), zwanego dalej „rozporządzeniem (UE) nr 2016/679”, z wyłączeniem 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 słuzówki 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 14 grudnia 2018 r. 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.

<sup>9)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

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 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 niejawnny, 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 wycisków ze słuzówki 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.”;

6) 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 wykrywania przestępstw oraz ścigania ich sprawców albo w celu ratowania życia i zdrowia ludzkiego.”;

7) 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.”;

8) 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 słuzówki 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”;

9) 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 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania.

Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy Straży Granicznej lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowiązaniu funkcjonariuszy Straży Granicznej lub 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.”;

10) w art. 98 ust. 3 otrzymuje brzmienie:

„3. Do służby, o której mowa w ust. 2 pkt 2, zalicza się również okresy służby oraz okresy równorzędne ze służbą w rozumieniu przepisów o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin.”.

**Art. 60.** W ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2018 r. poz. 2214) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 2018 r. poz. 2129 i 2161 oraz z 2019 r. poz. 83) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 2018 r. poz. 2033) w art. 39 po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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. z 2018 r. poz. 2216 oraz z 2019 r. poz. 15) 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.<sup>10)</sup>) 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. 1d i 1e ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.<sup>11)</sup>);”.

<sup>10)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 685, 771, 1000, 1356, 1629, 1637 i 2348 oraz z 2019 r. poz. 42.

<sup>11)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544, 1669, 2077, 2102, 2245 i 2399 oraz z 2019 r. poz. 15, 53, 81 i 125.



**Art. 66.** W ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652, 1010, 1387 i 2432) 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.”;

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 2018 r. poz. 1921) 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.<sup>12)</sup>), 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 ust. 2 rozporządzenia 2016/679 w Biuletynie Informacji Publicznej na stronie podmiotowej 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;

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 i 2399) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 oraz z 2018 r. poz. 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 2019 r. poz. 44) wprowadza się następujące zmiany:

1) tytuł ustawy otrzymuje brzmienie:

„o przetwarzaniu informacji kryminalnych”;

<sup>12)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

## 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 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);”;

## 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.”;

## 9) tytuł rozdziału 4 otrzymuje brzmienie:

„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.<sup>13)</sup>), zwanej dalej „ustawą o Policji”, lub 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.<sup>14)</sup>), 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 lub 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”.

**Art. 71.** W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2019 r. poz. 52, 55 i 60) 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 urzędnicy 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 szczególnie 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.<sup>15)</sup>), 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 ust. 2 rozporządzenia 2016/679 w Biuletynie Informacji Publicznej na stronie podmiotowej 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 w zakresie działalności sądu:

- 1) rejonowego – prezes sądu okręgowego;
- 2) okręgowego – prezes sądu apelacyjnego;
- 3) 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;

<sup>13</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544, 1669, 2077, 2102, 2245 i 2399 oraz z 2019 r. poz. 15, 53, 81 i 125.

<sup>14</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 106, 138, 650, 730, 894, 1544 i 2399 oraz z 2019 r. poz. 53 i 125.

<sup>15</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

- 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);
- 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 14 grudnia 2018 r. 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 rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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, 650, 1544 i 2399 oraz z 2019 r. poz. 53) 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.”;
- 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 lub dane genetyczne, o których mowa w art. 4 pkt 2 i 4 ustawy z dnia 14 grudnia 2018 r. 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 obowiązane 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 dotyczy, 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 słuzówki 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 słuzówki 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 słuzówki 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 2019 r. poz. 58 i 60) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 oraz z 2019 r. poz. 125).”;

- 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jest Główny Inspektor Transportu Drogowego lub wojewódzki inspektor transportu drogowego.”.

**Art. 74.** W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2018 r. poz. 2387, 2245 i 2399 oraz z 2019 r. poz. 53) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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 2018 r. poz. 2107) 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.<sup>16)</sup>), 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 ust. 2 rozporządzenia 2016/679 w Biuletynie Informacji Publicznej na stronie podmiotowej oraz w widocznym miejscu w budynku sądu.

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 Naczelnny 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, z późn. zm.<sup>17)</sup>) 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 i 2448) 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.<sup>18)</sup>);”.

**Art. 78.** W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2018 r. poz. 2104 i 2399 oraz z 2019 r. poz. 53) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku

<sup>16)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

<sup>17)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2361 oraz z 2018 r. poz. 650, 927, 1338, 1629 i 2245.

<sup>18)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544, 1669, 2077, 2102, 2245 i 2399 oraz z 2019 r. poz. 15, 53, 81 i 125.

z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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, z późn. zm.<sup>19)</sup>) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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. 2162 i 2354) 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 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 jakiegokolwiek 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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.<sup>20)</sup>.”;

2) tytuł rozdziału 2 otrzymuje brzmienie:

„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

<sup>19)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 650, 1544, 1669 i 2399 oraz z 2019 r. poz. 53.

<sup>20)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.



osób przez granice (kodeks graniczny Schengen) (Dz. Urz. UE L 77/1 z 23.03.2016) przysługuje Straży Granicznej i Służbie Celno-Skarbowej;”;

4) 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 ust. 2 w pkt 1, 5 i 9 oraz w art. 28 w różnej liczbie i w różnym przypadku wyraz „wykorzystywania” zastępuje się użytym w odpowiedniej liczbie i przypadku wyrazem „przetwarzania”;

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

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 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 2018 r. poz. 1870 oraz z 2019 r. poz. 61) 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 rozgrywanym 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 rozgrywanym 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:

„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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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. 22 ust. 1 pkt 1 lit. a i b 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. 22 ust. 1 pkt 1 lit. a i b 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 ust. 1 pkt 2 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 3–5 i 9;
- 4) art. 39 ust. 1 pkt 3 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 3 i 6–10;
- 5) art. 39 ust. 1 pkt 4 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 4 i 7;
- 6) art. 39 ust. 1 pkt 5 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 8 i 9;
- 7) art. 39 ust. 1 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, 1669, 2245 i 2399) 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, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125)

– 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 14 grudnia 2018 r. 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 i 1524 oraz z 2018 r. poz. 1115, 1515, 2219 i 2429).

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 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.<sup>21)</sup>), zwanego dalej „rozporządzeniem 2016/679”, w zakresie, w jakim przepisy szczególnie przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowiązaniu funkcjonariuszy lub 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,
  - dane 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,

<sup>21)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.



- 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 innych 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, 357, 398 i 650 oraz z 2019 r. poz. 55).

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 Prokuratury 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 danych 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 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 16 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 16 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 16 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) warunki, o których mowa w art. 25d ust. 1, 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) warunki, o których mowa w art. 25d ust. 2, w przypadku podmiotu wymienionego w art. 25c ust. 1 pkt 16;
- 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 określają, 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 oraz z 2019 r. poz. 125), w celu ich wymiany z organami ścigania innych państw na zasadach i w 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 z 2019 r. poz. 60) 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.<sup>22)</sup>) w art. 25 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) Komendant Główny Policji – 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.<sup>23)</sup>);”.

**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.”.

**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;”;

<sup>22)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 723, 730, 771, 1000 i 1104 oraz z 2019 r. poz. 55.

<sup>23)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405, z 2018 r. poz. 106, 138, 416, 650, 730, 1039, 1544, 1669, 2077, 2102, 2245 i 2399 oraz z 2019 r. poz. 15, 53, 81 i 125.

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;
- 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 bezpośrednią wymianę 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. 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) w art. 10 pkt 4 otrzymuje brzmienie:

„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.”;

- 7) tytuł rozdziału 3 otrzymuje brzmienie:  
„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 Unii Europejskiej, 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 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 o tym 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 należyтым 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 danych 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 niehumanitarnego traktowania lub karania.

3. Administrator danych dokumentuje fakt przekazania danych osobowych w przypadkach, o których mowa w ust. 2, oraz bez zbędnej zwłoki 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 danych 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. 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 niepełne 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) art. 26 otrzymuje brzmienie:

„Art. 26. W sprawach nieuregulowanych w niniejszej ustawie stosuje się przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).”.

**Art. 86.** W ustawie z dnia 11 września 2015 r. o zużytych 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).”.

**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 powszechnie jednostki organizacyjne prokuratury zgodnie z art. 13 § 6, wykonują w zakresie działalności prokuratury:

- 1) rejonowej – prokurator okręgowy;
- 2) okręgowej – prokurator regionalny;
- 3) 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 danych i podmiotów przetwarzających wiedzy o obowiązkach wynikających z ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);
- 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.<sup>24)</sup>), 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 14 grudnia 2018 r. 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 danych lub podmiotu przetwarzającego o podejrzeniu naruszenia przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 3) uzyskiwania od administratora danych i podmiotu przetwarzającego dostępu do wszelkich danych osobowych oraz informacji niezbędnych organowi nadzorczemu do realizacji jego zadań;
- 4) uzyskiwania dostępu do pomieszczeń administratora danych i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych;
- 5) wydawania ostrzeżeń administratorowi danych lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 6) udzielania upomnień administratorowi danych lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 7) wzywania administratora danych lub podmiotu przetwarzającego do dostosowania operacji przetwarzania danych do przepisów ustawy z dnia 14 grudnia 2018 r. 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).”.

<sup>24)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

**Art. 89.** W ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2018 r. poz. 508, z późn. zm.<sup>25)</sup>) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).”;

2) 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 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.”;

3) 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 z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na zasadach określonych w tej ustawie.

2. Danej 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 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.<sup>26)</sup>) mogą być przetwarzane przez organy KAS również dla celów określonych w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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.”;

4) 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 14 grudnia 2018 r. 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.<sup>27)</sup>), 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 ust. 2 rozporządzenia 2016/679 w Biuletynie Informacji Publicznej na stronie podmiotowej oraz w widocznym miejscu w budynku Trybunału.

<sup>25)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 723, 1000, 1039, 1499, 1544, 1577, 1654, 2193, 2245 i 2354 oraz z 2019 r. poz. 53.

<sup>26)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

<sup>27)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

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, 1499 i 2193) 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, nie stosuje się przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) 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 2018 r. poz. 2268) 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 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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.<sup>28)</sup>) 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.<sup>29)</sup>), 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 ust. 2 rozporządzenia 2016/679 w Biuletynie Informacji Publicznej na stronie podmiotowej 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, z późn. zm.<sup>30)</sup>) wprowadza się następujące zmiany:

1) w art. 3 w pkt 3 po wyrazach „funkcjonariuszy i pracowników” dodaje się wyraz „SOP”;

2) w art. 6 w ust. 2 pkt 1 otrzymuje brzmienie:

„1) przekazują SOP wszelkie informacje, w tym dane osobowe, mogące mieć wpływ na bezpieczeństwo ochraniających osób lub obiektów;”;

<sup>28)</sup> Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 771, 847, 848, 1045, 1443 i 2507.

<sup>29)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

<sup>30)</sup> Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 650, 730, 1544, 1562, 1669, 2245 i 2399.

- 3) w art. 51 skreśla się zdanie drugie;
- 4) w art. 56:
  - a) w ust. 6 pkt 1 otrzymuje brzmienie:

„1) dane osobowe, o których mowa w art. 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);”;
  - 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;
- 5) 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.”;
- 6) uchyla się art. 60;
- 7) art. 61 otrzymuje brzmienie:

„Art. 61. Administratorem danych osobowych przetwarzanych przez SOP jest Komendant SOP.”;
- 8) 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 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.<sup>31)</sup>), zwanego dalej „rozporządzeniem (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 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych osobowych po pisemnym zobowiązaniu funkcjonariuszy lub pracowników do zachowania przetwarzanych danych w poufności.”.

**Art. 95.** W ustawie z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej (Dz. U. poz. 729, 1669 i 2399) wprowadza się następujące zmiany:

  - 1) w art. 3 dodaje się ust. 6–8 w brzmieniu:

„6. Do pracowników Straży Marszałkowskiej, o których mowa w ust. 5, stosuje się odpowiednio przepisy art. 21 ust. 1, 2, 4, art. 22 ust. 1, art. 23 ust. 1, art. 24, art. 27–29, art. 30 ust. 1a–3 oraz art. 48 ust. 1a pkt 3 oraz ust. 1b i 1c ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. z 2018 r. poz. 1915).

7. Uprawnienia kierowników urzędów przewidziane w art. 48 ust. 1a pkt 3 oraz ust. 1b i 1c ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych w odniesieniu do pracowników Straży Marszałkowskiej, o których mowa w ust. 5, wykonuje Komendant Straży Marszałkowskiej.

8. Regulamin wynagradzania pracowników Straży Marszałkowskiej, o których mowa w ust. 5, zatwierdza Marszałek Sejmu.”;
  - 2) 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;
  - 3) 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 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

<sup>31)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

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.<sup>32)</sup>), zwanego dalej „rozporządzeniem (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 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy Straży Marszałkowskiej lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowiązaniu funkcjonariuszy Straży Marszałkowskiej lub pracowników do zachowania przetwarzanych danych w poufności.”;

4) w art. 42 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Rada Ministrów określi, w drodze rozporządzenia, równorzędność stopni w formacjach, o których mowa w ust. 1, mając na względzie zapewnienie adekwatności tych stopni w służbach, o których mowa w ust. 1, oraz w odniesieniu do żołnierzy zawodowych.”;

5) użyty w art. 67 ust. 15, w art. 68 ust. 2 i w art. 73 ust. 1 wyraz „powołaniem” zastępuje się wyrazem „mianowaniem”;

6) w art. 86 w ust. 2 w pkt 1 we wprowadzeniu do wyliczenia wyrazy „art. 83” zastępuje się wyrazami „art. 85”;

7) w art. 126 w ust. 4 wyrazy „ust. 1” zastępuje się wyrazami „ust. 3”.

**Art. 96.** W ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. poz. 723, 1075, 1499 i 2215) wprowadza się następujące zmiany:

1) w art. 96 ust. 3 otrzymuje brzmienie:

„3. Dane, o których mowa w art. 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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. 97.** 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 oraz z 2019 r. poz. 125);”;

b) uchyla się ust. 2;

<sup>32)</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

- 4) w art. 59 w ust. 1 pkt 2 otrzymuje brzmienie:
- „2) sprawuje nadzór nad zgodnością przetwarzania danych PNR przez JIP z przepisami niniejszej ustawy oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);”;
- 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 14 grudnia 2018 r. 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 14 grudnia 2018 r. 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. 98.** 1. Osoba pełniąca w dniu wejścia w życie niniejszej ustawy funkcję inspektora ochrony danych osobowych na podstawie przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669), 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 inspektora ochrony danych osobowych, o którym mowa w ustawie z dnia 10 maja 2018 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. 99.** 1. Do kontroli wszczętych na podstawie przepisów 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) 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. 100.** 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. 101.** Podmiot, do którego przed dniem wejścia w życie niniejszej 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. 102.** 1. W terminie 1 roku od dnia wejścia w życie niniejszej 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 wskazany 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, 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. 103.** 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. 104.** 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. 102 ust. 3.

**Art. 105.** 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. 29 ust. 8 ustawy zmienianej w art. 72,
- 5) art. 42 ust. 6 ustawy zmienianej w art. 81,
- 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, art. 20 ust. 1n i art. 20 ust. 1o ustawy zmienianej w art. 58, w brzmieniu nadanym niniejszą ustawą,
- 2) art. 10a ust. 18 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. 29 ust. 17 ustawy zmienianej w art. 72, w brzmieniu nadanym niniejszą ustawą,
- 5) art. 42 ust. 6 ustawy zmienianej w art. 81, 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. 106.** 1. Maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy wynosi w:

- 1) 2019 r. – 1 250 000 zł;
- 2) 2020 r. – 1 350 000 zł;
- 3) 2021 r. – 1 380 000 zł;
- 4) 2022 r. – 1 410 000 zł;
- 5) 2023 r. – 1 450 000 zł;
- 6) 2024 r. – 1 490 000 zł;
- 7) 2025 r. – 1 530 000 zł;
- 8) 2026 r. – 1 570 000 zł;
- 9) 2027 r. – 1 610 000 zł;
- 10) 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. 107.** 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 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 uchyłającą 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.

**Art. 108.** Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:

- 1) art. 58 pkt 12, który wchodzi w życie z dniem 1 listopada 2019 r.;
- 2) art. 82 pkt 5 w zakresie art. 25c–25h, które wchodzi w życie po upływie roku od dnia ogłoszenia.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*