Projekt z dnia 18 kwietnia 2018 r.

U S T A W A

z dnia <data wydania aktu>r.

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

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawa określa:

1) zasady i warunki ochrony danych osobowych przetwarzanych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu;
2) prawa osób, których dane osobowe są przetwarzane, w celach o których mowa w pkt 1, oraz środki ochrony prawnej przysługujące tym osobom;

---

1) Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L z 4.5.2016, str. 89).

2) Niniejszą ustawą zmienia się następujące ustawy: ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, 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 29 sierpnia 1997 r. o strażach gminnych, ustawę z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, ustawę z dnia 8 października 2004 r. o ustanowieniu Medalu za Zasługi dla Straży Granicznej, ustawę z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, ustawę z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, ustawę z dnia 9 kwietnia 2010 r. o Służbie Więziennej, ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, ustawę z dnia 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 8 grudnia 2017 r. o Służbie Ochrony Państwa, ustawę z dnia 10 stycznia 2018 r. o szczególnych rozwiązaniach związanych z organizacją w Rzeczypospolitej Polskiej sesji Konferencji Stron Ramowej konwencji Narodów Zjednoczonych w sprawie zmian klimatu, ustawę z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej.

3) sposób prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych w celach, o których mowa w pkt 1, z wyłączeniem danych osobowych przetwarzanych przez prokuraturę i sądy.

2. Przepisów ustawy nie stosuje się do ochrony danych osobowych:

1) znajdujących się w aktach, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, spraw i czynności prowadzonych na podstawie ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2016 r. poz. 1654 oraz z 2017 r. poz. 773), ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652), ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2017 r. poz. 1904, 2405 oraz z 2018 r. poz. 5, 106, 138 i 201), ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475), ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396 oraz z 2016 r. poz. 2205), ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5) oraz wydanych na ich podstawie aktów wykonawczych;
2) znajdujących się w Rejestrze Sprawców Przestępstw na Tle Seksualnym prowadzonym na podstawie przepisów ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym (Dz. U. z 2018 r. poz. 405);
3) wymienianych z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, Agencją Unii Europejskiej do spraw Współpracy Organów Ścigania (Europol), Europejską Jednostką Współpracy Sądowej (Eurojust) oraz organizacjami międzynarodowymi;
4) znajdujących się we wpisach do Systemu Informacyjnego Schengen;
5) znajdujących się we wpisach do Wizowego Systemu Informacyjnego;
6) znajdujących się we wpisach do system wjazdu/wyjazdu (EES);
7) 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. 2. 1. Ustawę stosuje się do przetwarzania danych osobowych w sposób:

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

2. Zautomatyzowany sposób przetwarzania polega na umieszczaniu danych w pamięci urządzenia i przetwarzaniu ich za pomocą opracowanego w tym celu programu informatycznego.

Art. 3. 1. W rozumieniu ustawy za dane osobowe uważa się informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, zwanej dalej „osobą, której dane dotyczą", przetwarzane w celach, o których mowa w art. 1 ust. 1 pkt 1.

2. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, adres zamieszkania lub zameldowania, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Art. 4. Ilekroć w ustawie jest mowa o:

1) administratorze – rozumie się przez to właściwy organ, który samodzielnie lub wspólnie z innym organem lub organami ustala cele i sposoby przetwarzania danych osobowych albo podmiot wskazany przez ustawę jako administratora danych osobowych;
2) danych biometrycznych – rozumie się przez to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
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, ujawniające 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 wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby;

5) 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;

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

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

8) organie nadzorczym 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;

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) organach ścigania państw członkowskich Unii Europejskiej – rozumie się przez to organy państw członkowskich Unii Europejskiej oraz państw niebędących państwami członkowskimi Unii Europejskiej stosujących przepisy dorobku Schengen, które są uprawnione w tych państwach do wykrywania i ścigania sprawców przestępstw lub przestępstw skarbowych oraz zapobiegania przestępczości i jej zwalczania;

11) organie właściwym – rozumie się przez to organ uprawniony na podstawie odrębnych ustaw do przetwarzania danych osobowych w celach, o których mowa w art. 1 ust. 1 pkt 1;

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

13) podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
14) profilowaniu – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na ich wykorzystaniu do oceny niektórych cech osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
15) przetwarzaniu – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, uzyskiwanie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
16) pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
17) wymianie – rozumie się przez to przekazywanie, udostępnianie, uzyskiwanie lub otrzymywanie informacji przez organy ścigania państw członkowskich Unii Europejskiej, państw trzecich lub agencje Unii Europejskiej i organizacje międzynarodowe zajmujące się zapobieganiem i zwalczaniem przestępczości oraz organy nadzorcze Unii Europejskiej, o których mowa w art. 48 oraz art. 49;
18) 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. Nie stanowią zbioru danych akta spraw, o których mowa w art. 1 ust. 2 pkt 1, również jeśli akta te, zawarte w nich dokumenty lub zapisy są tworzone lub przetwarzane z wykorzystaniem technik informatycznych.

Rozdział 2

Nadzór nad przetwarzaniem danych osobowych

Art. 5. 1. Prezes Urzędu Ochrony Danych Osobowych, zwany dalej „Prezesem Urzędu”, jest organem nadzorczym w rozumieniu art. 41 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016, str. 89).

2. Nadzór nad ochroną danych osobowych, sprawowany przez Prezesa Urzędu, nie obejmuje danych przetwarzanych w celach określonych w art. 1 ust. 1 pkt 1 przez prokuraturę i sądy.

Art. 6. 1. Do zadań Prezesa Urzędu realizowanych w zakresie określonym w art. 5 należy w szczególności:

1) monitorowanie i egzekwowanie stosowania przepisów niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych;
2) upowszechnianie wiedzy z zakresu stosowania niniejszej ustawy, w szczególności wśród administratorów i podmiotów przetwarzających;
3) 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 Unii Europejskiej;
4) rozpatrywanie zażaleń, o których mowa w art. 50;
5) sprawdzanie zgodności przetwarzania danych osobowych z przepisami niniejszej ustawy w przypadku zastosowania przez administratora art. 24 ust. 3 oraz informowanie osoby, której dane dotyczą, w terminie do 30 dni o wynikach tego sprawdzenia lub o powodach jego nieprzeprowadzenia;
6) prowadzenie postępowania w sprawie stosowania niniejszej ustawy, w tym na podstawie informacji otrzymanych od innego organu publicznego;
7) monitorowanie zmian mających wpływ na ochronę danych osobowych, w szczególności rozwój technologii informacyjno-komunikacyjnych;
8) pełnienie funkcji konsultacyjnych, o których mowa w art. 38, dotyczących operacji przetwarzania w ramach niniejszej ustawy.

2. Prezes Urzędu nieodpłatnie wykonuje swoje zadania na rzecz osoby, której dane dotyczą, lub inspektora ochrony danych, w zakresie, o którym mowa w niniejszej ustawie.

3. Jeżeli żądanie wykonania zadania jest w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swą powtarzalność, Prezes Urzędu może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na Prezesie Urzędu.

Art. 7. W celu wykonania zadań, o których mowa w art. 6 ust. 1 pkt 1 i 5–7, Prezes Urzędu może przeprowadzać kontrolę przetwarzania danych osobowych, zwaną dalej „kontrolą". Do prowadzenia kontroli stosuje odpowiednio przepisy rozdziału 9 ustawy z dnia ….. o ochronie danych osobowych (Dz. U. poz. …), z wyłączeniem art. 80 ust. 1 pkt 2, art. 85 ust. 4 i art. 86 tej ustawy.

Art. 8. 1. Administrator, podmiot przetwarzający lub odbiorca, zwani dalej „podmiotami kontrolowanymi", są obowiązani umożliwić kontrolującemu przeprowadzenie kontroli.

2. W toku kontroli kontrolujący ma prawo wglądu do zbioru danych, z zachowaniem przepisów ustawy o ochronie informacji niejawnych, jedynie w obecności upoważnionego przedstawiciela właściwego organu, w którym jest przeprowadzana kontrola oraz z wykorzystaniem jego kodów dostępowych do zbiorów danych, o ile są one stosowane. Kontrolujący ma również prawo wglądu do innych dokumentów i informacji mających bezpośredni związek z przedmiotem kontroli.

Art. 9. 1. W przypadku naruszenia przepisów o ochronie danych osobowych zbieranych w celach, o których mowa w art. 1 ust. 1 pkt 1, Prezes Urzędu – z urzędu lub na wniosek osoby zainteresowanej – 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.

2. W przypadku uzasadnionego podejrzenia naruszenia przepisów o ochronie danych osobowych przetwarzanych w celach, o których mowa w art. 1 ust. 1 pkt 1, Prezes Urzędu – z urzędu lub na wniosek osoby zainteresowanej – wydaje administratorowi lub podmiotowi przetwarzającemu ostrzeżenie, w którym wskazuje, iż planowane operacje przetwarzania mogą skutkować naruszeniem przepisów niniejszej ustawy.

3. Decyzje Prezesa Urzędu, o których mowa w ust. 1, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Administrator lub podmiot przetwarzający dane osobowe, o których mowa w zdaniu pierwszym, jest zobowiązany do niezwłocznego przywrócenia zgodnego z prawem sposobu ich przetwarzania.

Art. 10. Na decyzję Prezesa Urzędu, o której mowa w art. 9 ust. 1, przysługuje skarga do sądu administracyjnego.

Art. 11. 1. W celu realizacji zadań, o których mowa w art. 6 ust. 1 pkt 3 i 8, Prezes Urzędu może kierować wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych zbieranych w celach, o których mowa w art. 1 ust. 1 pkt 1.

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

Art. 12. 1. Prezes Urzędu może zwrócić się bezpośrednio do inspektora ochrony danych, o którym mowa w art. 46, o dokonanie sprawdzenia stosowania przepisów niniejszej ustawy przez administratora, który go powołał, wskazując zakres i termin tego sprawdzenia.

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

3. Dokonanie 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. 13. Postępowanie w sprawach uregulowanych w niniejszej ustawie prowadzi się według przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149 i 650), zwanej dalej „Kodeksem postępowania administracyjnego”, o ile przepisy niniejszej ustawy nie stanowią inaczej.

Rozdział 3

Zasady przetwarzania danych osobowych

Art. 14. 1. Właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

2. Dane osobowe mogą być przetwarzane wyłącznie w celach, o których mowa w art. 1 ust. 1 pkt 1.

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

4. Dopuszcza się przetwarzanie danych osobowych do innych celów, niż określone w art. 1 ust. 1 pkt 1, jeśli jest to niezbędne dla ochrony życia, zdrowia lub żywotnych interesów osoby, której dane dotyczą oraz jeżeli przepisy prawa lub prawo Unii Europejskiej zezwalają na ich przetwarzanie.

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

6. Do ochrony danych osobowych przetwarzanych w celach, o których mowa w ust. 4–5, zastosowanie mają przepisy ustawy z dnia …. o ochronie danych osobowych oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1).

Art. 15. 1. Niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych

genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej, zwanych dalej „danymi sensytywnymi”.

2. Dopuszcza się przetwarzanie danych sensytywnych, z wyłączeniem danych dotyczących seksualności i orientacji seksualnej, jeżeli:

1) jest to konieczne dla:
   a) osiągnięcia prawnie dopuszczalnych celów określonych w odrębnych przepisach,
   b) ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby;
2) dane takie zostały upublicznione przez osobę, której dane dotyczą.

Art. 16. 1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, mające dla niej niekorzystne skutki prawne lub poważnie na nią wpływające, wyłącznie w wyniku przetwarzania danych osobowych w sposób zautomatyzowany, w tym w wyniku profilowania, chyba że dopuszcza je prawo Unii Europejskiej lub odrębne przepisy, którym podlega administrator i które przewidują odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ze strony administratora.

2. Rozstrzygnięcia, o których mowa w ust. 1, nie mogą opierać się na danych sensytywnych, 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 sensytywnych, skutkującego dyskryminacją tych osób.

Art. 17. 1. Administrator dokonuje weryfikacji danych osobowych w terminach określonych przez przepisy szczególne, regulujące działania właściwego organu, a jeśli przepisy te nie określają terminu – nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych.

2. Weryfikacja dokonywana jest w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane usuwa się, z zastrzeżeniem art. 18.

Art. 18. Dane osobowe uznane za zbędne można przekształcić w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, iż przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań.

Art. 19. Jeżeli dane osobowe są przetwarzane w związku z dokumentowaniem czynności realizowanych przez właściwe organy, jako elektroniczna kopia akt kontrolnych, dane osobowe pozostawia się po ich zanonimizowaniu.

Art. 20. Przy przetwarzaniu danych osobowych, o ile rozróżnienie to jest niemożliwe lub dalece utrudnione, administrator zapewnia podział na dane osobowe dotyczące:

1) osób, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
2) osób skazanych za czyn zabroniony;
3) pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;
4) innych osób związanych z czynem zabronionym, takich jak: osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania; 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. 21. Przy przetwarzaniu danych osobowych administrator zapewnia podział na dane osobowe mające swe źródło w faktach i dane osobowe mające swe źródło w indywidualnych ocenach, z wyłączeniem przypadków, w których rozróżnienie to jest niemożliwe lub dalece utrudnione.

Art. 22. 1. Właściwy organ może przesyłać lub udostępniać dane osobowe innym właściwym organom, państwu trzeciemu lub organizacji międzynarodowej po uprzednim zweryfikowaniu prawidłowości, kompletności i aktualności tych danych oraz w sposób umożliwiający odbiorcy dokonanie ich oceny.

2. Właściwy organ przesyłając dane osobowe dodają niezbędne dodatkowe informacje pozwalające odbiorcy ocenić stopień prawidłowości, kompletności, wiarygodności oraz aktualności tych danych.

Art. 23. Właściwy organ, który przekazał nieprawdziwe, niekompletne lub nieaktualne dane osobowe lub przekazał te dane z naruszeniem przepisów niniejszej ustawy, jest obowiązany, bez zbędnej zwłoki, poinformować o tym odbiorcę oraz sprostować, uzupełnić lub uaktualnić te dane, przekazując dane właściwe albo usunąć lub ograniczyć ich przetwarzanie, chyba, że z uwagi na upływ czasu jest to oczywiście nieuzasadnione.

Rozdział 4

Prawa osoby, której dane dotyczą

Art. 24. 1. Osobie, której dane dotyczą przysługuje, z zastrzeżeniem przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412 i 650), prawo do uzyskania informacji od administratora o przetwarzaniu jej danych osobowych oraz do informacji o:

1) celu i podstawie prawnej ich przetwarzania;
2) rodzaju danych osobowych, które są przetwarzane, oraz informacjach o pochodzeniu tych danych;
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 zażalenia, o którym mowa w art. 50, oraz danych kontaktowych Prezesa Urzędu, z wyłączeniem spraw, o których mowa w art. 5 ust. 2;
7) prawie dostępu do jej danych osobowych.

2. W postępowaniu karnym i karno-skarbowym wykonywanie uprawnień, o których mowa w ust. 1, w art. 25 ust. 1 i art. 26 ust.1 podlega następującym ograniczeniom:

1) prawo dostępu osób, będących uczestnikami postępowania, do ich danych osobowych jest wykonywane przez dostęp do akt tego postępowania, zgodnie z przepisami, które taki dostęp regulują;
2) uprawnienia inne niż prawo dostępu do danych osobowych nie przysługują do czasu prawomocnego zakończenia postępowania;
3) po prawomocnym zakończeniu tego postępowania jego uczestnikom przysługują uprawnienia określone w ust. 1 i 4, art. 25 ust. 1 pkt 1–4, 6 i 7 oraz w art. 26 ust. 1.

3. Administrator nie przekazuje osobie, której dane dotyczą, informacji, o których mowa w ust. 1, jeżeli ich ujawnienie mogłoby spowodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;

2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karno-skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
4) zagrożenie dla życia, zdrowia ludzkiego lub bezpieczeństwa publicznego, lub porządku publicznego;
5) zagrożenie dla obronności lub bezpieczeństwa państwa;
6) zagrożenie dla podstaw ekonomicznych państwa;
7) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

4. Administrator może przekazać osobie, której dane dotyczą, informacje, o których mowa w ust. 1, w przypadku gdy ich ujawnienie byłoby niezbędne do ochrony jej żywotnych interesów lub innej osoby.

5. Informacje, o których mowa w ust. 1, są udzielane na wniosek. Administrator każdorazowo, z wyłączeniem przypadku, o którym mowa w ust. 2, udzielając odpowiedzi na wniosek o uzyskanie informacji poucza osobę, której dane dotyczą, o:
1) zasadach udostępniania informacji ze zbiorów danych;
2) możliwości wniesienia do Prezesa Urzędu zażalenia, o którym mowa w art. 50.

6. Organy prowadzące postępowanie karne lub karno-skarbowe pouczają strony i świadków o przetwarzaniu ich danych osobowych, a także celu i podstawie prawnej ich przetwarzania.

7. Administrator dokumentuje faktyczne lub prawne przyczyny odmowy lub ograniczenia przekazania całości lub części informacji. Informacje o przyczynach odmowy lub ograniczenia przekazania udostępnia Prezesowi Urzędu na jego wniosek.

Art. 25. 1. Osoba, której dane dotyczą, może wystąpić do administratora z wnioskiem o uzyskanie:
1) nazwy, adresu i danych kontaktowych administratora;
2) danych kontaktowych inspektora ochrony danych;
3) celów przetwarzania, do którego mają posłużyć dane osobowe;
4) informacji o prawie wniesienia do Prezesa Urzędu zażalenia, o którym mowa w art. 50, oraz danych kontaktowych Prezesa Urzędu;
5) informacji o możliwości wniesienia wniosku do administratora o udostępnienie, sprostowanie lub usunięcie danych osobowych, lub ograniczenie przetwarzania danych osobowych;

6) podstawy prawnej przetwarzania danych osobowych;
7) informacji o okresie przechowywania danych osobowych lub, gdy nie jest to możliwe, o kryteriach służących określeniu tego okresu;
8) kategoriach odbiorców danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych – jeżeli przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej ma miejsce.

2. Administrator nie przekazuje osobie danych, o których mowa w ust. 1 pkt 5–8, w sytuacjach, o których mowa w art. 24 ust. 3.

3. Administrator może przekazać osobie, której dane dotyczą, informacje o których mowa w ust. 1 pkt 5–8, w przypadku gdy ich ujawnienie byłoby niezbędne do ochrony jej żywotnych interesów lub innej osoby.

Art. 26. 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, znajdujące się w jawnych zbiorach danych osobowych, zostały zebrane z naruszeniem przepisów niniejszej ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane.

2. W razie uznania wniosku, o którym mowa w ust. 1, za zasadny administrator odpowiednio uzupełnia, aktualizuje lub sprostowuje dane osobowe, albo dokonuje ich usunięcia.

3. Administrator nie dokonuje uzupełnienia, aktualizacji, sprostowania albo usunięcia danych osobowych w sytuacjach, o których mowa w art. 24 ust. 3.

4. Administrator może dokonać uzupełnienia, aktualizacji, sprostowania albo usunięcia danych osobowych w przypadku gdy ich ujawnienie byłoby niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby.

5. Jeżeli osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić, lub gdy dane osobowe muszą zostać zachowane do celów dowodowych, administrator jest obowiązany, bez zbędnej zwłoki, do czasowego ograniczenia przetwarzania kwestionowanych danych.

6. W razie potwierdzenia prawidłowości danych osobowych, administrator – przed zniesieniem ograniczenia przetwarzania kwestionowanych danych – informuje o tym osobę, której dane dotyczą.

7. W razie niedopełnienia przez administratora obowiązku, o którym mowa w ust. 1, 5 oraz 6, osoba, której dane dotyczą, może się zwrócić do Prezesa Urzędu z wnioskiem o nakazanie dopełnienia tego obowiązku.

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

9. Administrator, bez zbędnej zwłoki, informuje odbiorców o dokonanym sprostowaniu lub usunięciu danych osobowych lub ograniczeniu ich przetwarzania, gdy czynności te dotyczyły danych nieprawidłowych, przetwarzanych niezgodnie z przepisami niniejszej ustawy lub w przypadku ograniczenia ich przetwarzania gdy ich prawidłowość jest kwestionowana.

10. W przypadku, o którym mowa w ust. 9, odbiorcy są zobowiązani do uaktualnienia, sprostowania lub usunięcia danych osobowych, lub wstrzymania ich przetwarzania.

11. Administrator pisemnie informuje osobę, której dane dotyczą, o każdej odmowie uaktualnienia, sprostowania lub usunięcia danych osobowych, lub ograniczenia ich przetwarzania, oraz o przyczynach tej odmowy.

12. Administrator nie informuje osoby, której dane dotyczą, o odmowie, o której mowa w ust. 11, w sytuacjach, o których mowa w art. 24 ust. 3.

13. W przypadku odmowy uaktualnienia, sprostowania lub usunięciu danych osobowych, lub czasowego ograniczenia ich przetwarzania – administrator poucza osobę, której dane dotyczą, o możliwości wniesienia zażalenia do Prezesa Urzędu, o którym mowa w art. 50.

Art. 27. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby, która złożyła wniosek na podstawie art. 25 ust. 1 i art. 26 ust. 1, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości tej osoby.

Art. 28. 1. W przypadkach, o których mowa w art. 24 ust. 3, art. 25 ust. 2 oraz art. 26 ust. 3, osoba, której dane dotyczą, może wystąpić do:

1) administratora z powtórnym wnioskiem, o którym odpowiednio mowa w art. 24 ust. 3, art. 25 ust. 1 oraz art. 26 ust. 1; albo
2) Prezesa Urzędu o weryfikację zasadności zastosowania przez administratora przesłanek, o których mowa w art. 24 ust. 2, art. 25 ust. 2 oraz art. 26 ust. 3.

2. Administrator informuje osobę, której dane dotyczą, o możliwości skorzystania z uprawnień, o których mowa w ust. 1.

3. Prezes Urzędu informuje osobę, której dane dotyczą, o wynikach przeprowadzonej weryfikacji, o której mowa w ust. 1 pkt 2, oraz o przysługującym jej prawie do wniesienia skargi do sądu administracyjnego.

Art. 29. 1. Administrator podejmuje działania mające na celu ułatwienie osobie, której dane dotyczą, wykonywanie przysługujących jej praw, o których mowa w art. 16 i 24–26.

2. Administrator udziela informacji, o których mowa w art. 24–26 osobie, której dane dotyczą, w takiej samej formie, w jakiej wniesiono wniosek, chyba że we wniosku zastrzeżono inną formę udzielenia informacji.

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

4. Czynności podejmowane przez administratora przy realizacji wniosków złożonych przez osoby, których dane dotyczą, na podstawie art. 24–26 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są nieuzasadnione ze względu na ich powtarzalność, administrator może:

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

5. Wysokość opłaty, o której mowa w ust. 4 pkt 1, wynosi 0,002 przeciętnego wynagrodzenia w poprzednim kwartale, począwszy od pierwszego dnia następnego miesiąca po ogłoszeniu przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie art. 20 pkt 2 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2017 r. poz. 1383, 1386, 2120 oraz z 2018 r. 138 i 357) za udostępnienie informacji.

6. 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. 30. 1. Administrator zapewnia, aby dane osobowe były:

1) rzetelne i przetwarzane zgodne z prawem 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) proporcjonalne do celów, dla których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;
5) przechowywane w formie umożliwiającej identyfikacje osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

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 prawidłową realizację czynności, o których mowa w ust. 1–2 i art. 14, oraz jest obowiązany do prowadzenia dokumentacji dotyczącej realizacji tych czynności. Dopuszcza się prowadzenie tej dokumentacji w postaci elektronicznej.

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

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

Art. 31. 1. Administrator, w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, stosuje odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, które zostały zaprojektowane w celu skutecznej realizacji zasad ochrony

danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by 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 przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla każdego konkretnego celu przetwarzania. Obowiązek ten ma zastosowanie do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te mają zapewnić, by domyślnie dane osobowe nie były udostępniane bez interwencji osoby fizycznej nieokreślonej liczbie osób fizycznych.

Art. 32. 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 porozumienia podział swoich obowiązków w zakresie:
   a) realizacji przez osobę, której dane dotyczą, przysługujących jej praw na mocy niniejszej ustawy,
   b) udzielania informacji, o których mowa w art. 25 ust. 1;
2) wyznaczają punkt kontaktowy dla osób, których dane dotyczą, w celu realizacji obowiązku, o którym mowa w pkt 1 lit. a.

Art. 33. 1. Administrator może w drodze umowy powierzyć przetwarzanie danych osobowych innemu podmiotowi, zwanemu dalej „podmiotem przetwarzającym”.

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

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

1) przedmiot i czas trwania przetwarzania;
2) charakter i cel przetwarzania;
3) rodzaj przetwarzanych danych osobowych;
4) kategorie osób, których dane dotyczą;
5) prawa i obowiązki administratora;

6) obowiązki podmiotu przetwarzającego, o których mowa w ust. 5;
7) sposób prowadzenia przez administratora kontroli przetwarzania.

4. Umowę powierzenia, o której mowa w ust. 1, sporządza się w 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 poleceniami administratora;
3) zapewnić, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności, również w zakresie środków technicznych ich zabezpieczenia;
4) 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 lub prawo Unii Europejskiej wymagają przechowywania danych osobowych;
5) udostępniać administratorowi wszelkie informacje związane z weryfikację prawidłowości realizacji umowy powierzenia, o której mowa w ust. 1;
6) współpracować z innymi podmiotami przetwarzającymi – w razie zawarcia przez administratora więcej niż jednej umowy powierzenia, o której mowa w ust. 1.

6. Podmiot przetwarzający może powierzyć przetwarzanie danych innemu podmiotowi przetwarzającemu każdorazowo wyłącznie na podstawie pisemnego upoważnienia administratora.

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 umową.

8. Jeżeli podmiot przetwarzający naruszy warunki umowy powierzenia, o której mowa w ust. 1, w zakresie celów lub sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Art. 34. 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. 32 ust. 1,
   c) inspektora ochrony danych;
2) cele przetwarzania;
3) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
4) opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych;
5) informacje o stosowaniu profilowania – w przypadku gdy zostało ono zastosowane;
6) kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
7) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;
8) planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe;
9) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, 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 nazwa oraz dane kontaktowe:
   a) podmiotu przetwarzającego,
   b) każdego administratora, w imieniu którego działa podmiot przetwarzający,
   c) inspektora ochrony danych;
2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
3) przypadki przekazania danych osobowych do państw trzecich lub organizacji międzynarodowej, w razie jednoznacznego polecenia administratora, łącznie z nazwą tego państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 39, w miarę możliwości.

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

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

Art. 35. 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 może być 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 przeznaczone są 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. 36. Administrator oraz podmiot przetwarzający współpracują z Prezesem Urzędu przy realizacji jego ustawowych zadań.

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.

Art. 38. 1. Administrator lub podmiot przetwarzający – przed rozpoczęciem przetwarzania danych osobowych, które będzie częścią mającego powstać nowego zbioru danych – występują do Prezes 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 przekazać właściwym organom dodatkowy wykaz operacji przetwarzania, które wymagają konsultacji z Prezesem Urzędu przed przystąpieniem do ich wykonywania.

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, stanowiłoby naruszenie przepisów niniejszej ustawy, w szczególności jeżeli uzna, że administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – w terminie do sześciu tygodni od dnia otrzymaniu wniosku o konsultacje, o którym mowa w ust. 1 – przedstawia administratorowi lub podmiotowi przetwarzającemu pisemne zalecenia. Prezes Urzędu może także skorzystać z przysługujących mu uprawnień, o których mowa w art. 9.

5. Z uwagi na złożony charakter sprawy, termin, o którym mowa w ust. 4, możne zostać przedłużony o miesiąc, o czym Prezesa 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.

Oddział 2

Zabezpieczenie danych osobowych

Art. 39. 1. Administrator i podmiot przetwarzający stosują środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, które w szczególności mają na celu:

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

2. Administrator i podmiot przetwarzający niszczą informatyczne nośniki danych wykorzystywane do przetwarzania danych osobowych wycofane z eksploatacji. Nośniki wycofane z eksploatacji nie mogą być zbywane.

Art. 40. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych w danym zbiorze danych nadane przez administratora lub podmiot przetwarzający. Zatwierdzony przez administratora wniosek o nadanie uprawnień do dostępu do zbioru danych osobowych uznaje się za nadanie takiego upoważnienia.

Art. 41. Administrator zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru danych wprowadzone oraz komu są przekazywane.

Art. 42. 1. Administrator 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 informatycznym.

2. Rolę ewidencji, o której mowa w ust. 1, może pełnić wykaz osób uprawnionych, prowadzony na podstawie zatwierdzonych przez administratora wniosków o nadanie uprawnień do dostępu do zabioru danych, o których mowa w art. 40.

Art. 43. Osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby 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 sporządza i przekazuje Prezesowi Urzędu uzasadnienie niedotrzymania tego terminu.

3. Podmiot przetwarzający – po stwierdzeniu naruszenia ochrony danych osobowych – bez zbędnej zwłoki zgłasza je administratorowi.

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

1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wykazów danych osobowych, których dotyczy naruszenie;
2) imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego podmiotu, 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.

7. Prezes Urzędu może przeprowadzać kontrolę realizacji przez administratora obowiązku, o którym w ust. 1–4.

8. W przypadku gdy naruszenie ochrony danych osobowych dotyczy 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.

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 stosował 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, wskazane w ust. 1;
3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku.

4. W przypadku, o którym mowa w ust. 3 pkt 3, zostaje wydany publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

5. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych, Prezes Urzędu – biorąc pod uwagę prawdopodobieństwo, że naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może:
1) zażądać wystosowania przez administratora zawiadomienia;
2) stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

6. W przypadku, o którym mowa w art. 25 ust. 1 pkt 5, 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. 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 oraz prowadzenie audytów przestrzegania niniejszej ustawy oraz innych przepisów dotyczących ochrony danych przez administratora oraz osoby zajmujące się przetwarzaniem;
4) realizowanie 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.

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

4. Inspektorem ochrony informacji może być osoba, która:

1) posiada wykształcenie wyższe;
2) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
3) posiada odpowiednią wiedzę i doświadczenie zawodowe w zakresie ochrony danych osobowych;
4) nie była skazana prawomocnym wyrokiem, orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.

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

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

7. Administrator zapewnia odpowiednie i niezwłoczne włączenie inspektora ochrony danych we wszystkie sprawach dotyczących ochrony danych osobowych.

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

9. Administrator przekazuje Prezesowi Urzędu dane kontaktowe inspektora ochrony danych oraz publikuje je na stronie internetowej.

10. Prezes Rady Ministrów określi, w drodze rozporządzenia tryb i sposób realizacji zadań, o których mowa w ust. 2, uwzględniając konieczność zapewnienia prawidłowości realizacji zadań inspektora ochrony danych oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.

Art. 47. 1. Inspektor ochrony danych sporządza i przekazuje administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdanie z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych znajdujących się w zbiorach danych administratora.

2. Sprawozdanie powinno zawierać:

1) imię i nazwisko inspektora ochrony danych;
2) wykaz czynności podjętych przez inspektora ochrony danych w toku sprawdzenia, o którym mowa w art. 12 ust. 1, oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
3) datę rozpoczęcia i zakończenia sprawdzenia, o którym mowa w art. 12 ust. 1;
4) określenie przedmiotu i zakresu sprawdzenia, o którym mowa w art. 12 ust. 1;
5) opis stanu faktycznego stwierdzonego w toku sprawdzenia, o którym mowa w art. 12 ust. 1, oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania z przepisami niniejszej ustawy;
6) stwierdzone przypadki naruszenia przepisów niniejszej ustawy w zakresie objętym sprawdzeniem, o którym mowa w art. 12 ust. 1, wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
7) wyszczególnienie załączników stanowiących składową część sprawozdania;
8) podpis inspektora ochrony danych, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy inspektora ochrony danych na każdej stronie sprawozdania;
9) datę i miejsce podpisania sprawozdania przez inspektora ochrony danych.

Rozdział 6

Współpraca z organami nadzorczymi Unii Europejskiej

Art. 48. 1. Prezes Urzędu udziela pomocy organom nadzorczym 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, by 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 Unii Europejskiej, od którego wniosek pochodzi, o odmowie realizacji wniosku oraz przedstawia powody odmowy.

6. Prezes Urzędu informuje organ nadzorczy 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 Unii Europejskiej, od którego wniosek pochodzi, w formie elektronicznej w uzgodnionym formacie.

8. Prezes Urzędu nie pobiera od organu nadzorczego 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 Unii Europejskiej mogą uzgodnić zasady wzajemnej rekompensaty wydatków poniesionych w wyniku realizacji konkretnego wniosku o pomoc.

Art. 49. 1. Prezes Urzędu może występować do organów nadzorczych Unii Europejskiej z wnioskiem o pomoc.

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

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

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

Rozdział 7

Środki ochrony prawnej i odpowiedzialność prawna

Art. 50. 1. Osobie, której prawa zostały naruszone w wyniku przetwarzania danych osobowych, przysługuje prawo wniesienia zażalenia do Prezesa Urzędu.

2. Prezes Urzędu udziela osobie, która wniosła zażalenie, dalszej pomocy na jej wniosek.

3. Zażalenie można wnieść również za pomocą elektronicznego formularza zamieszczonego na stronie internetowej Prezesa Urzędu.

4. Prezes Urzędu informuje osobę, która wniosła zażalenie, o postępach w jego wyjaśnianiu, sposobie jego rozpatrzenia oraz możliwości wniesienia wniosku o ponowne rozpatrzenie sprawy.

5. Prezes Urzędu nie przekazuje osobie, która wniosła zażalenie, informacji mogących wskazywać na przetwarzanie danych osobowych przez organy właściwe, w sytuacjach o których mowa w art. 24 ust. 3.

Art. 51. 1. Osoba, której dane dotyczą, może zwrócić się do Prezesa Urzędu z wnioskiem o ponowne rozpatrzenie sprawy w terminie 14 dni od dnia otrzymania decyzji albo pisemnej informacji, o której mowa w art. 24. Do wniosku stosuje się odpowiednio przepisy Kodeksu postępowania administracyjnego dotyczące odwołania.

2. Wniosek o ponowne rozpatrzenie sprawy jest opiniowany przez Prezesa Urzędu w terminie 30 dni od dnia, w którym Prezes Urzędu otrzymał wniosek.

3. Prezes Urzędu pisemnie informuje osobę, która wystąpiła z wnioskiem o ponowne rozpatrzenie sprawy, o sposobie jego rozstrzygnięcia.

4. Opinia dotycząca wniosku o ponowne rozpatrzenie sprawy nie może być sporządzana przez osobę, która uprzednio oceniała lub opiniowała zaskarżane rozstrzygnięcie.

Art. 52. 1. Każdej osobie, której dane dotyczą, przysługuje prawo do wniesienia na decyzje Prezesa Urzędu skargi do sądu administracyjnego.

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

3. Do rozpatrywania skarg stosuje się przepisy ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2017 r. poz. 1369, 1370 i 2451 oraz z 2018 r. poz. 650), z tym że:

1) przekazanie akt i odpowiedzi na skargę następuje w terminie 15 dni od dnia otrzymania skargi;
2) skargę rozpatruje się w terminie 30 dni od dnia otrzymania akt wraz z odpowiedzią na skargę.

Art. 53. 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. 54. Osobie, która poniosła szkodę w wyniku operacji przetwarzania danych osobowych niezgodnej z prawem lub w wyniku czynności naruszającej przepisy niniejszej ustawy, przysługuje od administratora odszkodowanie.

Rozdział 8

Przepisy karne

Art. 55. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2. Jeśli czyn określony w ust. 1 dotyczy danych sensytywnych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Art. 56. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat dwóch.

Rozdział 9

Przepisy zmieniające

Art. 57. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067 i 2405 oraz z 2018 r. poz. 106 i 138) wprowadza się następujące zmiany:

1) w art. 14:
   a) w ust. 1 w pkt 1 po wyrazie „przestępstw” dodaje się przecinek i wyrazy „przestępstw skarbowych”,
   b) w ust. 4 wyrazy „ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) zastępuje się wyrazami „ustawy z dnia …… o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …)”;
2) w art. 15 w ust. 1:
   a) 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;”;

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

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

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, 3a lit. b–d, 3b i 5–7, oraz wzory dokumentów stosowanych w tych sprawach, mając na względzie zapewnienie skuteczności działań podejmowanych przez Policję oraz poszanowanie praw osób, wobec których działania te są podejmowane. ”;

3) 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–1r w brzmieniu:

„1a. Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może dotyczyć danych osobowych, o których mowa w art. 15 ust. 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przy czym dane dotyczące wyników analizy kwasu deoksyrybonukleinowego (DNA) obejmują informacje wyłącznie o niekodującej części DNA.

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

1c. Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do realizacji zadań ustawowych lub wykonywania uprawnień związanych z prowadzeniem postępowań administracyjnych, realizacją czynności administracyjno-porządkowych oraz innych czynności, do przeprowadzania których funkcjonariusze Policji są uprawnieni na podstawie ustaw, w celach innych niż określone w art.1 ust. 1 pkt 1 ustawy z dnia …. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych

w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1), zwanego dalej „rozporządzeniem (UE) 2016/679”, z wyłączeniem danych dotyczących kodu genetycznego.

1d. Dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia (UE) 2016/679, mogą być przetwarzane wyłącznie, gdy jest to niezbędne ze względu na zakres lub charakter prowadzonego postępowania administracyjnego lub dokonywanych czynności realizowanych na podstawie ustaw.

1e. W celu realizacji zadań ustawowych Policja jest uprawniona do nieodpłatnego uzyskiwania informacji, w tym danych osobowych, od innych służb, instytucji państwowych oraz organów władzy publicznej. Służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia Policji informacji, w tym danych osobowych. W szczególności Policja jest uprawniona do uzyskiwania informacji, w tym danych osobowych:

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

1f. Służby, instytucje państwowe oraz organy władzy publicznej administrujące zbiorami danych lub rejestrami, o których mowa w ust. 1e pkt 1, mogą wyrazić zgodę na udostępnianie za pomocą urządzeń telekomunikacyjnych informacji zgromadzonych w tych zbiorach lub rejestrach – jednostkom organizacyjnym Policji, bez konieczności składania pisemnych wniosków, jeżeli jednostki te:

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.

1g. 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 w stosunku do zbiorów danych osobowych utworzonych przez nich w celu realizacji zadań ustawowych.

1h. Kierownicy jednostek organizacyjnych Policji, o których mowa w ust. 1g, 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.

1i. 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. 1g, z czego sporządza się protokół.

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

1k. Dane osobowe przetwarza się przez okres niezbędny do wykonania ustawowych zadań przez Policję, jeżeli odrębne przepisy dotyczące przetwarzania danych osobowych nie stanowią inaczej. Kierownicy jednostek organizacyjnych Policji, o których mowa w ust. 1g, dokonują weryfikacji tych danych nie rzadziej niż co 10 lat od dnia ich uzyskania.

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

1m. Przetwarzanie danych osobowych przez Policję w celu innym niż wskazany w ust. 1l, odbywa się na zasadach określonych w rozporządzeniu (UE) 2016/679.

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

1o. Policja pobiera odciski linii papilarnych lub wymazy ze śluzówki policzków od funkcjonariuszy i pracowników Policji wykonujących służbowe

czynności związane z ujawnianiem, zabezpieczaniem lub badaniem śladów związanych z podejrzeniem popełnienia czynu zabronionego – w celach wyeliminowania pozostawionych przez nich śladów.

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

1q. 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.

1r. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory kart daktyloskopijnych, na których dane daktyloskopijne są pobierane przez upoważnione podmioty i przekazywane Komendantowi Głównemu Policji w celu przetwarzania w zbiorach danych daktyloskopijnych, oraz tryb i sposób ich przekazywania Komendantowi Głównemu Policji przez zobowiązane do tego służby, instytucje państwowe oraz organy władzy publicznej – uwzględniając charakter realizowanych zadań i celów przeznaczenia danej karty daktyloskopijnej.”;

c) w ust. 2a po pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 i 9 w brzmieniu:

„8) osobach, wobec których zastosowano środki ochrony i pomocy, przewidziane w ustawie z dnia 25 czerwca 1997 r. o świadku koronnym (Dz. U. z 2016 r. poz. 1197);

9) pokrzywdzonych, których dane są przetwarzane na podstawie przepisów odrębnych.”,

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 organów sądowniczych, międzynarodowych organów ścigania oraz w Międzynarodowej Organizacji Policji Kryminalnej – Interpol, za zgodą tych osób. Policja przekazując wyniki przetwarzania zastrzega, iż nie udostępnia się ich osobie, której dane osobowe dotyczą.”;

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

„1) dane osobowe, o których mowa w art. 15 ust. 1 ustawy z dnia ……. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z tym że dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA;”,

f) uchyla się ust. 2c,

g) w ust. 4 dodaje się zdanie trzecie w brzmieniu: „Informacje i dane udostępnia się także organom ścigania państw członkowskich Unii Europejskiej, agencjom Unii Europejskiej zajmującymi się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol, jeżeli następuje to w celu ścigania karnego.”,

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

i) uchyla się ust. 15–19;

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

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

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

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

c) po ust. 7 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 zajmującymi się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol na ich wniosek, jeżeli następuje to w celu ścigania karnego albo w celu ratowania życia lub zdrowia ludzkiego.”;

6) w art. 20cb:

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

b) ust. 2 otrzymuje brzmienie:

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

7) 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”;

8) 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. poz. 1635, z 2014 r. poz. 1877 i 1915 oraz z 2017 r. poz. 60).”;

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

„Art. 20f. 1. W związku z obsługą zadań, o których mowa w art. 20e ust. 1 pkt 1, Komendant Główny Policji przetwarza w SWD Policji informacje, w tym dane osobowe,

osób których dane uzyskano w związku z realizacją zadań, o których mowa w art. 1 ust. 2 i 3, i w tym zakresie jest administratorem w rozumieniu przepisów o ochronie danych osobowych.

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

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

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

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

10) art. 21a–21e otrzymują brzmienie:

„Art. 21a. 1. Komendant Główny Policji prowadzi zbiór danych zawierający informacje o wynikach analizy kwasu deoksyrybonukleinowego (DNA), zwany dalej „zbiorem danych DNA”, którego jest administratorem w rozumieniu ustawy z dnia …… o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

2. W zbiorze danych DNA przetwarza się:

1) informacje, w tym dane osobowe, o których mowa w ust. 1, w odniesieniu do:
   a) osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego,
   b) nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego,
   c) osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi

stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396 oraz z 2016 r. poz. 2205),

d) osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904 i 1948),

e) oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego,

f) osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość,

g) zwłok ludzkich o nieustalonej tożsamości,

h) śladów nieznanych sprawców przestępstw,

i) osób zaginionych,

j) osób, o których mowa w art. 15 ust. 1 pkt 3a lit. c,

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

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. 1o 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. k są przetwarzane w zbiorze danych DNA w celu wyeliminowania – spośród wszystkich zebranych w toku prowadzonego postępowania – śladów pozostawionych przez osoby, o których mowa w art. 20 ust. 1o.

Art. 21e. 1. W weryfikacji, o której mowa w art. 17 ustawy z dnia …… o ochronie danych osobowych przetwarzanych w związku zapobieganiem i zwalczaniem przestępczości, uczestniczą jednostki organizacyjne Policji, służby, instytucje państwowe lub organy władzy publicznej, które przekazały informacje, w tym dane osobowe, do zbioru danych DNA.

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

1) zostało umorzone postępowanie z uwagi na to, że:

a) czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia,

b) zdarzenie lub okoliczność, w związku z którymi wprowadzono dane osobowe do zbioru danych , nie ma znamion czynu zabronionego;

2) osoba, której dane dotyczą:

a) została uniewinniona prawomocnym wyrokiem sądu,

b) ukończyła 100. rok życia,

c) zmarła;

3) tożsamość zwłok ludzkich została ustalona;

4) utracą swoją przydatność identyfikacyjną, 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, 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.”;

11) uchyla się art. 21f i 21g;

12) art. 21h–21n otrzymują brzmienie:

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

1) Centralną Registraturę Daktyloskopijną, w której są gromadzone karty daktyloskopijne i chejroskopijne zawierające odciski linii papilarnych osób;

2) zbiór automatycznie przetwarzający dane daktyloskopijne, w którym są przetwarzane informacje, w tym dane osobowe, o odciskach linii papilarnych osób, niezidentyfikowanych śladach linii papilarnych z miejsc przestępstw oraz śladach linii papilarnych, które mogą pochodzić od osób zaginionych

– zwane dalej łącznie „zbiorami danych daktyloskopijnych”.

2. W zbiorach danych daktyloskopijnych są przetwarzane:

1) informacje, w tym dane osobowe, dotyczące:
   a) osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego,
   b) nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego,
   c) osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób,
   d) osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych,
   e) oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego,
   f) osób poszukiwanych,
   g) cudzoziemców, od których zostały pobrane odciski linii papilarnych w sytuacjach, o których mowa w art. 35 ust. 2, art. 324 pkt 1, art. 394 ust. 3 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach 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. 1o.
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. 20 ust. 1o, są przechowywane w zbiorach danych daktyloskopijnych i wykorzystywane w celu prowadzenia czynności identyfikacyjnych.

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

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

Art. 21l. 1. W weryfikacji, o której mowa w art. 17 ustawy z dnia ……. .. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, uczestniczą jednostki organizacyjne Policji, służby, instytucje państwowe lub organy władzy publicznej, które przekazały informacje, w tym dane osobowe, do zbiorów danych daktyloskopijnych.

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

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

13) po art. 21n dodaje się art. 21na–21nc w brzmieniu:

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

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

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

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

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

5. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, parametry funkcjonalne KSIP, sposób jego funkcjonowania, w tym w sytuacjach awaryjnych oraz sposób utrzymania, mając na uwadze potrzebę zapewnienia optymalnego poziomu jego funkcjonowania.”.

14) 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 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. 12–22 i art. 34 rozporządzenia (UE) 2016/679.

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.

4. Zasady i warunki przetwarzania informacji, w tym danych osobowych w celach, o których mowa w ust. 1, określa:

1) ustawa z dnia …. o ochronie danych osobowych;

2) rozporządzenie (UE) 2016/679 – z zastrzeżeniem, o którym mowa w ust. 2

5. Wyłączenia, o których mowa w ust. 2, stosuje się w przypadku informacji, w tym danych osobowych, niezbędnych do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień wynikających z ustawy.

6. Informacje, w tym dane osobowe, o których mowa w ust. 1, przetwarza się przez okres niezbędny do wykonania ustawowych zadań przez Policję. Administrator danych dokonuje weryfikacji tych danych nie rzadziej niż co 10 lat od dnia uzyskania informacji.”;

14) 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 zmieniające 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 190 z 29.6.2013, str. 1), zwane 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. 58. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2017 r. poz. 2365 i 2405 oraz z 2018 r. poz. 106 i 138) 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. 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 postepowania karnego, a także wykonują czynności na polecenie sądu i prokuratury oraz innych właściwych organów państwowych w zakresie, w jakim obowiązek ten został określony w odrębnych przepisach.”,

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

c) w ust. 7 pkt 5 otrzymuje brzmienie:

„5) sposób i tryb przetwarzania informacji, w tym danych osobowych, gromadzonych przez Straż Graniczną w ramach wykonywanych zadań, w zakresie nieobjętym innymi przepisami wydanymi na podstawie ustawy;”;

3) 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. 15 ust. 1 ustawy z dnia ……. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przy czym dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA.

3. Danych osobowych, o których mowa w art. 15 ust. 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej w prowadzonym postępowaniu.

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

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

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

6. Dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwanego dalej „rozporządzeniem (UE) nr 2016/679”, mogą być przetwarzane wyłącznie, gdy jest to niezbędne ze względu na zakres lub charakter prowadzonego postępowania administracyjnego, dokonywanych kontroli lub czynności realizowanych na podstawie ustaw.

7. Straż Graniczna podejmując działania na podstawie informacji, w tym danych osobowych, przetwarzanych przez Międzynarodową Organizację Policji Kryminalnej – Interpol może wystąpić o przekazanie informacji uzupełniających, w zakresie

umożliwiającym wykonanie tych działań. Wymiana informacji uzupełniających odbywa się za pośrednictwem komórki organizacyjnej Komendy Głównej Policji wyznaczonej do wykonywania zadań Krajowego Biura Interpolu.

8. Straż Graniczna, w zakresie swojej właściwości, przetwarza informacje, w tym dane osobowe, uzyskane ze zbiorów danych prowadzonych przez inne służby, instytucje państwowe oraz organy władzy publicznej. Służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia Straży Granicznej informacji, w tym danych osobowych.

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 pisemnego wniosku, jeżeli jednostki te spełniają łącznie następujące warunki:

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

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

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

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

13. Komendant Główny Straży Granicznej może upoważnić osoby, o których mowa w ust. 11, 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. Dane osobowe przetwarza się przez okres niezbędny do wykonania ustawowych zadań przez Straż Graniczną, jeżeli odrębne przepisy dotyczące przetwarzania danych osobowych nie stanowią inaczej. Administrator danych dokonuje weryfikacji tych danych nie rzadziej niż co 10 lat od dnia ich uzyskania.

15. Przetwarzanie danych osobowych przez Straż Graniczną w celu, o którym mowa w art. 1 ust. 1 pkt 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na zasadach określonych w tej ustawie.

16. Przetwarzanie danych osobowych przez Straż Graniczą w celu innym niż wskazany w ust. 15, odbywa się na zasadach określonych w rozporządzeniu (UE) 2016/679, z wyłączeniem przepisów art. 12–22 oraz art. 34 rozporządzenia (UE) 2016/679.

17. Wyłączenia, o których mowa w ust. 16, 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.

18. Straż Graniczna udostępnia właściwym podmiotom informacje, o których mowa w art. 1 ust. 2 pkt 9, w tym dane osobowe, na pisemny wniosek, 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.

19. Przepisu ust. 18 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.

20. 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 na taki sposób udostępnienia informacji, w tym danych osobowych.

21. Minister właściwy do spraw wewnętrznych w porozumieniu z Ministrem Sprawiedliwości określi, w drodze rozporządzenia, sposób pobierania wymazów ze

śluzówki policzków, gromadzenia odcisków linii papilarnych oraz zdjęć sygnalitycznych osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, osób o nieustalonej tożsamości lub osób usiłujących ukryć swą 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 przez nieuprawnionym dostępem.”;

4) w art. 10b:

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

b) po ust. 7 dodaje się ust. 8 w brzmieniu:

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

5) 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.”;

6) w art. 11:

a) w ust. 1 po pkt 5b dodaje się pkt 5c–5e w brzmieniu:

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

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

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

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

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

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 4–5e, 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.”;

7) 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 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. 12–22 i art. 34 rozporządzenia (UE) 2016/679.

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

Art. 59. W ustawie z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (Dz. U. poz. 491, z późn. zm.[3)]) wprowadza się następujące zmiany w art. 11t:

1) po ust. 7 dodaje się ust. 7a i 7b w brzmieniu:

„7a. Przetwarzanie danych osobowych przez Biuro w celach, o którym mowa w art. 1 ust. 1 pkt 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. ……), odbywa się na zasadach określonych w tej ustawie.

7b. Przetwarzanie danych osobowych przez Biuro w celach innych niż wskazane w ust. 7a, odbywa się na zasadach określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), z wyłączeniem przepisów art. 12–22 oraz art. 34 tego rozporządzenia.”;

2) w ust. 8 po wyrazie „Wewnętrznego” dodaje się przecinek i wyrazy „z zastrzeżeniem ograniczeń określonych we właściwych przepisach o ochronie danych osobowych”;

3) w ust. 9 wyrazy „5 lat” zastępuje się wyrazami „10 lat”.

Art. 60. W ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2017 r. poz. 220, z późn. zm.[4)]) w art. 28b pkt 8 otrzymuje brzmienie:

„8) Policji – jeżeli jest to konieczne do skutecznego zapobieżenia popełnieniu przestępstwa, jego wykrycia albo ustalenia sprawców i uzyskania dowodów, na zasadach i w trybie określonych w art. 20 ust. 1e i 1f ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067 i 2405 oraz z 2018 r. poz. 106 i 138);”.

Art. 61. W ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652) 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

---

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

4) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 791, 1089, 1387 i 1566 oraz z 2018 r. poz. 8, 138, 317 oraz 650).

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. 62. W ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z 2016 r. poz. 706 oraz z 2017 r. poz. 60 i 2405) dotychczasową treść art. 10a oznacza się jako ust. 1 i dodaje się ust. 2–7 w brzmieniu:

„2. Administratorem danych osobowych przetwarzanych przez straż jest komendant straży.

3. Przetwarzanie danych osobowych przez straż w celach, o którym mowa w art. 1 ust. 1 pkt 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. ……), odbywa się na zasadach określonych w tej ustawie.

4. Przetwarzanie danych osobowych przez straż w celach innych niż wskazane w ust. 3, odbywa się na zasadach określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), z wyłączeniem przepisów art. 12–22 oraz art. 34 tego rozporządzenia.

5. Dane osobowe przetwarzane są przez okres niezbędny do realizacji ustawowych zadań straży, z zastrzeżeniem ograniczeń określonych we właściwych przepisach o ochronie danych osobowych.

6. Komendant straży dokonuje weryfikacji danych osobowych nie rzadziej, niż co 10 lat od dnia ich zebrania, uzyskania, pobrania lub aktualizacji, usuwając zbędne dane.

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

Art. 63. W ustawie z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (Dz. U. z 2018 r. poz. 424) wprowadza się następujące zmiany:

1) w tytule ustawy ogólne określenie przedmiotu ustawy otrzymuje brzmienie:

„o przetwarzaniu informacji kryminalnych”;

2) art. 1 i 2 otrzymują brzmienie:

„Art. 1. Ustawa określa zasady postępowania przy przetwarzaniu i przekazywaniu 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 i przekazuje w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania i zwalczania przestępczości zapobiegania i zwalczania przestępczości.

2. Informacje kryminalne przetwarza się i przekazuje 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 aniżeli określone w ust. 1, w zakresie niezbędnym dla ich 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:

a) po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) administrator – oznacza administratora w rozumieniu art. 4 pkt 1 ustawy z dnia …….. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …..);”,

b) pkt 4 otrzymuje brzmienie:

„4) przetwarzanie informacji kryminalnych – oznacza przetwarzanie w rozumieniu art. 4 pkt 15 ustawy, o której mowa w pkt 1a;”;

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 informacji kryminalnych, w tym danych osobowych, przetwarzanych na zasadach określonych w niniejszej ustawie.”;

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, o której mowa w art. 4 pkt 1a oraz przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r. poz. 1167 i 1948, z 2017 r. poz. 935 oraz z 2018 r. poz. 106 i 138).”;

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) art. 18 otrzymuje brzmienie:

„Art. 18. 1. Przetwarzanie i przekazywanie informacji kryminalnych podlega kontroli Prezesa Urzędu Ochrony Danych Osobowych.

2. W zakresie nieuregulowanym w niniejszej ustawie do przetwarzania i przekazywania informacji kryminalnych stosuje się przepisy ustawy, o której mowa w art. 4 pkt 1a.”;

9) tytuł rozdziału 4 otrzymuje brzmienie:

„Rozdział 4

Przetwarzanie, przekazywanie 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 i 2405 oraz z 2018 r. poz. 106 i 138), zwanej dalej „ustawą o Policji", oraz organu Straży Granicznej, o którym mowa w art. 3c ust. 2 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2017 r. poz. 2365 i 2405 oraz 2018 r. poz. 106 i 138), zwanej dalej „ustawą o Straży Granicznej", w przypadku udostępnienia informacji kryminalnej w zakresie realizacji zadań ustawowych określonych w art. 5b ust. 1 ustawy o Policji i art. 3c ust. 1 ustawy o Straży Granicznej przepisu ust. 1 nie stosuje się.";

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

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

Art. 64. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2018 r. poz. 430 i 650), wprowadza się następujące zmiany art. 29 otrzymuje brzmienie:

„Art. 29. 1. Żandarmeria Wojskowa, w celu realizacji zadań ustawowych jest uprawniona do przetwarzania i wymiany informacji, w tym danych osobowych.

2. Żandarmeria Wojskowa przetwarza informacje, w tym dane osobowe, w:

1) Komendzie Głównej Żandarmerii Wojskowej w zakresie danych przetwarzanych przez wszystkie jednostki i komórki organizacyjne Żandarmerii Wojskowej;

2) jednostkach i komórkach organizacyjnych Żandarmerii Wojskowej – w zakresie ich właściwości rzeczowej.

3. Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może mieć charakter niejawny oraz odbywać się bez zgody i wiedzy osoby, której te informację dotyczą.

4. Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może odbywać się z wykorzystaniem środków technicznych, w tym teleinformatycznych.

5. Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może dotyczyć danych osobowych, o których mowa w art. 15 ust. 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), przy czym dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA.

6. Danych osobowych, o których mowa w art. 15 ust. 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej w prowadzonym postepowaniu.

7. W celu realizacji zadań ustawowych Żandarmeria Wojskowa jest uprawniona do nieodpłatnego uzyskiwania informacji, w tym danych osobowych, od innych służb, instytucji państwowych oraz organów władzy publicznej. Administratorzy danych tych podmiotów są obowiązani do nieodpłatnego ich udostępniania, na podstawie imiennego upoważnienia Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, okazanego przez żołnierza Żandarmerii Wojskowej, wraz z legitymacją służbową. Fakt udostępnienia tych danych podlega ochronie na podstawie przepisów o ochronie informacji niejawnych. W szczególności Żandarmeria Wojskowa jest uprawniona do uzyskiwania informacji, w tym danych osobowych:

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

8. Służby, instytucje państwowe oraz organy władzy publicznej administrujące zbiorami danych lub rejestrami, o których mowa w ust. 7 udostępniają w drodze teletransmisji informacje zgromadzone w tych zbiorach lub rejestrach – jednostkom organizacyjnym Żandarmerii Wojskowej, bez konieczności składania pisemnych wniosków, jeżeli jednostki te:

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 lub uprawnień albo prowadzonej działalności.

9. Komendant Główny Żandarmerii Wojskowej jest administratorem danych osobowych przetwarzanych przez Żandarmerię Wojskową w celu realizacji ustawowych zadań.

10. Dane osobowe przetwarza się przez okres niezbędny do wykonania ustawowych zadań lub uprawnień przez Żandarmerię Wojskową, jeżeli odrębne przepisy dotyczące przetwarzania danych osobowych nie stanowią inaczej. Kierownicy właściwych jednostek organizacyjnych Żandarmerii Wojskowej dokonują weryfikacji tych danych nie rzadziej niż co 10 lat od chwili ich uzyskania.

11. Przetwarzanie danych osobowych przez Żandarmerię Wojskową w celu zapobiegania i zwalczania przestępczości odbywa się na zasadach określonych w ustawie z dnia …… o ochronie danych osobowych przetwarzanych do celów zapobiegania i zwalczania przestępczości, prawie Unii Europejskiej oraz postanowieniach umów międzynarodowych.

12. Przetwarzanie danych osobowych przez Żandarmerię Wojskową w celu innym niż wskazany w ust. 10, odbywa się na zasadach określonych w rozporządzeniu (UE) 2016/679, z wyłączeniem przepisów art. 12–22 oraz art. 34 rozporządzenia (UE) 2016/679.

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

14. Minister Obrony Narodowej określi, w drodze rozporządzenia:

1) zasady przetwarzania informacji, w szczególności danych biometrycznych oraz przypadki ich pobierania.
2) zbiory danych, w których te dane będą przetwarzane.
3) wzory dokumentów obowiązujących przy przetwarzaniu tych danych oraz sposób ich oceny pod kątem ich przydatności w prowadzonych postępowaniach, uwzględniając przy tym potrzebę ich ochrony przed nieuprawnionym dostępem;
4) przesłanki zaniechania zbierania określonych rodzajów informacji;
5) wzór upoważnienia, o którym jest mowa w ust. 7, uwzględniając niezbędne dane żołnierza Żandarmerii Wojskowej.”.

Art. 65. W ustawie z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz. U. z 2018 r. poz. 473) w art. 104 w ust. 1 pkt 10 otrzymuje brzmienie:

„10) Policji, o ile są niezbędne w toczącym się postępowaniu lub na potrzeby wykonywania czynności operacyjno-rozpoznawczych na zasadach i w trybie określonym w art. 20 ust. 1e i 1f ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067 i 2405 oraz z 2018 r. poz. 106 i 138);”.

Art. 66. W ustawie z dnia 8 października 2004 r. o ustanowieniu Medalu za Zasługi dla Straży Granicznej (Dz. U. poz. 2662) art. 11 otrzymuje brzmienie:

„Art. 11. Przechowywanie w ewidencji danych dotyczących podstawy decyzji o pozbawieniu Medalu, o których mowa w art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), nie wymaga zgody osoby, której dane dotyczą.”.

Art. 67. W ustawie z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. z 2018 r. poz. 134 i 138) wprowadza się następujące zmiany:

1) w art. 2:

a) pkt 18 otrzymuje brzmienie:

„18) wykorzystywaniu danych – rozumie się przez to przetwarzanie danych będących danymi osobowymi w rozumieniu rozporządzenia 2016/679, jak również jakiekolwiek operacje wykonywane na danych niebędących danymi osobowymi, takie jak zbieranie, wpisywanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;”,

b) po pkt 18 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 4.05.2016, str. 1).”;

2) art. 8–10 otrzymują brzmienie:

„Art. 8. 1. Prezes Urzędu Ochrony Danych Osobowych sprawuje nadzór nad tym, czy wykorzystywanie danych nie narusza praw osób, których dane te dotyczą.

2. Prezes Urzędu Ochrony Danych Osobowych jest uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu sprawowania nadzoru, o której mowa w ust. 1.

3. Nadzór, o którym mowa w ust. 1, jest sprawowany zgodnie z przepisami ustawy z dnia …….. o ochronie danych osobowych (Dz. U. poz. …).

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. Centralny organ techniczny KSI, w zakresie wykorzystywania danych poprzez Krajowy System Informatyczny (KSI), jest administratorem danych w rozumieniu art. 4 pkt 7 rozporządzenia 2016/679.”;

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

„2. Do wykorzystywania danych SIS i VIS nie stosuje się przepisów art. 12–22 i art. 34 rozporządzenia 2016/679 w zakresie w jakim jest to niezbędne do realizacji celów określonych w art. 23 ust. 1 lit. a, c, d oraz i rozporządzenia 2016/679. Administrator odmawiając osobie, której dane dotyczą prawa do dostępu do danych SIS lub danych VIS jest obowiązany poinformować o ograniczeniach w wykorzystywaniu danych SIS i VIS niezwłocznie nie później niż w terminie 60 dni od otrzymania wniosku o dostęp do danych.”;

4) w art. 25 ust. 3 otrzymuje brzmienie:

„3. Minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii Prezesa Urzędu Ochrony Danych Osobowych określi, w drodze rozporządzenia, sposób przeprowadzania szkoleń z zakresu bezpieczeństwa i ochrony danych wykorzystywanych

poprzez Krajowy System Informatyczny (KSI) oraz kwalifikacje osób uprawnionych do przeprowadzania tych szkoleń, uwzględniając konieczność zapewnienia ochrony danych.”.

Art. 68. W ustawie z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. z 2017 r. poz. 1160 oraz z 2018 r. poz. 138 i 310) wprowadza się następujące zmiany:

1) w art.1 pkt 4 otrzymuje brzmienie:

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

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 wprowadza się następujące zmiany:

a) ust. 2b i 2c otrzymują brzmienie:

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

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

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

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

c) ust. 7–14 otrzymują brzmienie:

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

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

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

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

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

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

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

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

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

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

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

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

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

5) w art. 15:
   a) w ust. 1 po wyrazie „danych” dodaje się wyraz „osobowych”;
   b) w ust. 2 po wyrazie „dane” dodaje się wyraz „osobowe”.
6) tytuł rozdziału 7 otrzymuje brzmienie:

„Rozdział 7

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

7) art. 35 otrzymuje brzmienie:

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

2. Przetwarzanie danych osobowych odbywa się zgodnie z przepisami o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości 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, zgodnie z przepisami ustawy z dnia …….. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …..);
5) współpraca z podmiotami zagranicznymi w zakresie, o którym mowa w pkt 1–3.”;

10) w art. 38:

a) w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie

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

b) ust. 2 i 3 otrzymują brzmienie:

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

3. Komendanci wojewódzcy (Komendant Stołeczny) Policji i komendanci powiatowi (rejonowi, miejscy) Policji przekazują podmiotom, o których mowa

w ust. 1 pkt 1–15, na wniosek tych podmiotów, informacje, w tym dane osobowe, o których mowa w art. 36 ust. 2 i art. 40, dotyczące imprez masowych organizowanych na obszarze działania tych komendantów. Przepisy art. 42 ust. 1, 4 i 5, art. 43, art. 44 ust. 1, 2 i 4, art. 45, art. 46 oraz art. 47 stosuje się odpowiednio.”;

11) art. 39 otrzymuje brzmienie:

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

2. Podmioty zobowiązane przekazują komendantom wojewódzkim (Komendantowi Stołecznemu) Policji i komendantom powiatowym (rejonowym, miejskim) Policji, na wniosek komendantów, informacje, w tym dane osobowe, o których mowa w art. 36 ust. 2 i art. 40, dotyczące imprez masowych organizowanych na obszarze działania tych komendantów. Przepisy art. 41, art. 42 ust. 1–3 oraz art. 45 stosuje się odpowiednio.”;

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

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

13) art. 41-43 otrzymują brzmienie:

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

2. Podmioty zobowiązane, o których mowa w:

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

5) art. 39 pkt 4 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 4 i 7;
6) art. 39 pkt 5 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 8 i 9;
7) art. 39 pkt 6 – przekazują informacje, w tym dane osobowe, o których mowa w art. 40 pkt 4, 8 i 9.

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

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

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

4. Komendant udziela informacji na kartach odpowiedzi.

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

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

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

2. Jeżeli zapytanie nie zawiera uzasadnienia lub jest ono niewystarczające, Komendant zwraca się do podmiotu uprawnionego, o którym mowa w ust. 1, o uzupełnienie stosownych informacji w tym danych osobowych.

3. W przypadku gdy zgromadzone przetwarzane w bazie 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 której 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 usunięciu ze bazy 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.”.

Art. 69. W ustawie z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. z 2017 r. poz. 631 i 1321 oraz z 2018 r. poz. 138) 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) w art. 18 w ust. 2 pkt 6 otrzymuje brzmienie:

„6) Prezes Urzędu Ochrony Danych Osobowych;”;

3) art. 24 otrzymuje brzmienie:

„Art. 24. 1. Służba Więzienna, w celu realizacji zadań, o których mowa w art. 2 ust. 1–2b, 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 sensytywnych, w rozumieniu ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …)

– niezbędnych do realizacji tych zadań.

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

przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z wyjątkami określonymi w niniejszej ustawie.

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

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

1) obecnie lub uprzednio pozbawionych wolności w zakładach karnych i aresztach śledczych – w zakresie związanym z pozbawieniem wolności w tych zakładach i aresztach, w tym w zakresie niezbędnym do:
   a) wykonania orzeczenia, zgodnie z zasadami określonymi w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
   b) zapewnienia porządku i bezpieczeństwa w zakładach karnych i aresztach śledczych,
   c) ochrony społeczeństwa przed przestępczością,
   d) wykonania zadań wynikających z odrębnych ustaw;
2) które mają być pozbawione wolności w zakładach karnych i aresztach śledczych, w wykonaniu orzeczenia wydanego przez właściwy organ, i przesłanego przez sąd do zakładu karnego lub aresztu śledczego, w celu realizacji czynności, o których mowa w art. 79 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy – w zakresie niezbędnym do wykonania orzeczenia, zgodnie z zasadami określonymi w tym kodeksie;
3) wobec których kary, środki karne i środki zabezpieczające są wykonywane w systemie dozoru elektronicznego – w zakresie niezbędnym do wykonania zadania, o którym mowa w art. 2 ust. 2a;
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) 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 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.”;

4) po art. 24 dodaje się art. 24a–24c w brzmieniu:

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

2. Służba Więzienna, na pisemny i uzasadniony wniosek osoby najbliższej, 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).

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. Zasady i warunki przetwarzania danych osobowych na podstawie niniejszej ustawy przez Służbę Więzienną w innych celach niż określone w art. 24 ust. 2 reguluje ustawa z dnia ..... o ochronie danych osobowych (Dz. U. poz. ….). oraz 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 4.05.2016, str. 1), zwane dalej „rozporządzeniem 2016/679”.

2. Do przetwarzania danych osobowych, o których mowa w art. 24 ust. 4, na potrzeby:

1) archiwizacji w interesie publicznym – przepisów art. 15 i art. 16 oraz art. 18–21 rozporządzenia 2016/679 nie stosuje się;
2) wykorzystania do celów naukowych, historycznych lub statystycznych – przepisów art. 15, art. 16, art. 18 i art. 21 rozporządzenia 2016/679 nie stosuje się.

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

1) danych osobowych w celu realizacji uprawnień wynikających z podległości służbowej i sprawowanego nadzoru, a także przeprowadzania kontroli organów Służby Więziennej i jednostek organizacyjnych, o których mowa w art. 7 i art. 8 ust.

1, na podstawie przepisów ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. poz. 1092);

2) 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. 5 ust. 2, art. 12–14, art.17 i art. 34 rozporządzenia 2016/79.

3. Informacji dotyczących danych osobowych funkcjonariuszy oraz pracowników nie udziela się na wniosek osadzonych lub osób prywatnych.

4. Dane osobowe, o których mowa w ust. 1, podlegają zabezpieczeniom przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustaw oraz zmianą, utratą, uszkodzeniem lub zniszczeniem i są przechowywane wyłącznie przez okres niezbędny do realizacji zadań, z tym że okres przechowywania tych danych osobowych ustala administrator zgodnie z celami ich przetwarzania, biorąc pod uwagę przepisy odrębne.

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

5) uchyla się art. 25;

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

„Rozdział 4a

Centralna Baza

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

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

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

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

b) informacje pozwalające na identyfikację osoby pozbawionej wolności, w tym dane biometryczne,
c) informacje wynikające z orzeczeń i innych dokumentów przesłanych przez sąd do zakładu karnego lub aresztu śledczego, w tym informacje, o których mowa w art. 11 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
d) informacje dotyczące stawienia się skazanego lub ukaranego do odbycia kary we właściwym zakładzie karnym lub areszcie śledczym,
e) informacje dotyczące osoby pozbawionej wolności zebrane w trybie art. 14 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
f) informacje związane z pobytem osoby pozbawionej wolności w zakładzie karnym lub areszcie śledczym, w szczególności:
   - informacje o wprowadzonych do wykonania orzeczeniach oraz okresach wykonywania pozbawienia wolności, w tym także poza zakładem karnym lub aresztem śledczym, oraz inne informacje mające wpływ na ustalenie terminu końca kary lub środka przymusu,
   - informacje niezbędne do dokonania prawidłowej klasyfikacji, rozmieszczenia wewnątrz zakładu karnego lub aresztu śledczego oraz indywidualnego postępowania zmierzającego do realizacji celów, jakim ma służyć wykonanie kar pozbawienia wolności, środków przymusu skutkujących pozbawieniem wolności oraz tymczasowego aresztowania, w tym w szczególności informacje:
     – – o których mowa w art. 82 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
     – – wynikające z badań osobopoznawczych, o których mowa w art. 82 § 3 i art. 212c § 1 zdanie pierwsze ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
     – – dotyczące diagnoz psychologicznych oraz udzielonej pomocy psychologicznej i terapeutycznej,
   - informacje o zakwalifikowaniu osoby pozbawionej wolności, jako osoby stwarzającej poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu karnego lub aresztu śledczego,
   - informacje o objęciu osoby pozbawionej wolności szczególną ochroną w warunkach zwiększonej izolacji i zabezpieczenia,

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

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

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

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

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

Art. 25b. 1. Dyrektor Generalny:

1) prowadzi w systemie teleinformatycznym Centralną Bazę;
2) jest administratorem informacji 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, iż przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań;

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

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

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

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

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

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

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

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

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

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

1) posiadają urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie informacje uzyskał;
2) posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie informacji niezgodnie z celem ich uzyskania;
3) jest to uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności;
4) po stronie tych podmiotów oraz Służby Więziennej istnieją warunki techniczne.

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

1) że informacje z Centralnej Bazy udostępniane są Rzecznikowi Praw Obywatelskich lub osobie przez niego upoważnionej na terenie zakładu karnego lub aresztu śledczego;
2) konieczność wprowadzenia zabezpieczeń technicznych i organizacyjnych uniemożliwiających wykorzystanie informacji niezgodnie z celem ich uzyskania;
3) zasady przetwarzania informacji w Centralnej Bazie przez Służbę Więzienną.

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

Art. 25e. Dyrektor Generalny, po wyrażeniu zgody w drodze decyzji, o której mowa w art. 25d ust. 1, umożliwia wielokrotne, nieograniczone w czasie udostępnianie informacji z Centralnej Bazy, w zakresie w określonym w tej decyzji, za pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku.

Art. 25f. 1. Dyrektor Generalny, w drodze decyzji, odmawia wyrażenia zgody na wielokrotne, nieograniczone w czasie, udostępnianie informacji z Centralnej Bazy, za

pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku, jeżeli:

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

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

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

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

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

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

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

1) wymagania, o których mowa w art. 25d ust. 1 pkt 1–4, w tym zwłaszcza konieczność wykazania przez podmioty, o których mowa w art. 25c ust. 1 pkt 3–14 i ust. 2, informacji, których udostępnianie jest niezbędne dla wykonywania zadań

określonych w odrębnych ustawach, oraz konieczność wykazania przez te podmioty odpowiedniego poziomu zabezpieczeń technicznych i organizacyjnych;

2) wymagania, o których mowa w art. 25d ust. 2, w przypadku podmiotu wymienionego w art. 25c ust. 1 pkt 15;

3) potrzebę zapewnienia sprawności i bezpieczeństwa udostępniania informacji z Centralnej Bazy, za pośrednictwem systemu teleinformatycznego, oraz ochrony tych informacji przed nieuprawnionym dostępem.

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

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

1) przekazuje, za pośrednictwem systemu teleinformatycznego, informacje o osobach pozbawionych wolności do Krajowego Rejestru Karnego, w zakresie określonym w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2017 r. poz. 678 i 1475 oraz z 2018 r. poz. 106, 138, 398 i 431) 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. 70. W ustawie z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz. U. z 2018 r. poz. 470) w art. 25 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) Komendant Główny Policji – na zasadach i w trybie określonym w art. 20 ust. 1e i 1f ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2017 r. poz. 2067 i 2405 oraz z 2018 r. poz. 106 i 138);”.

Art. 71. W ustawie z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym (Dz. U. poz. 1688 oraz z 2017 r. poz. 2056) w art. 2 w ust. 2 po pkt 10 kropkę zastępuje się średnikiem i dodaje się pkt 11 w brzmieniu:

„11) informatycznych nośników danych wykorzystywanych do przetwarzania danych osobowych, o których mowa w ustawie z dnia ……..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …).”.

Art. 72. W ustawie z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5) w art. 13 po § 5 dodaje się § 6 i 7 w brzmieniu:

„§ 6. Kierownicy powszechnych jednostek organizacyjnych prokuratury są administratorami danych osobowych przetwarzanych w ramach realizowanych zadań.

§ 7. Do przetwarzania danych osobowych w postępowaniach albo systemach teleinformatycznych w ramach realizacji zadań, o których mowa w ust. 2, przepisów art. 13–16 oraz 18–21 rozporządzenia 2016/679 nie stosuje się.”.

Art. 73. W ustawie z dnia 13 kwietnia 2016 r o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (Dz. U. z 2018 r. poz. 410) art. 9 otrzymuje brzmienie:

„Art. 9. Do danych osobowych zgromadzonych w systemie zgłaszania stosuje się przepisy ustawy z dnia… o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U…. poz….).”.

Art. 74. W ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2018 r. poz. 508 i 650) wprowadza się następujące zmiany:

1) w art. 35 dodaje się ust. 5 i 6 w brzmieniu:

„5. Do przetwarzania danych osobowych w CRDP stosuje się 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 4.5.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, z wyłączeniem art. 12–22 i art. 34 tego rozporządzenia, z zastrzeżeniem ust. 6.

6. Do danych gromadzonych oraz przetwarzanych w CRDP w związku z zapobieganiem i zwalczaniem przestępczości stosuje się przepisy ustawy z dnia ……. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …).”;

2) w art. 45 ust. 1 otrzymuje brzmienie:

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

3) w art. 47:

a) w ust. 1:

– w pkt 2:

– – po lit. b dodaje się lit. ba w brzmieniu:

„ba) ustawie z dnia 21 listopada 1996 r. o muzeach,”,

– – po lit. d dodaje się lit. da w brzmieniu:

„da) ustawie z dnia 27 czerwca 1997 r. o bibliotekach,”,

– – po lit. l dodaje się lit. m w brzmieniu:

„m) ustawie z dnia 9 marca 2017 r. o systemie monitorowania drogowego przewozu towarów,”,

b) część wspólna otrzymuje brzmienie:

„– mogą przetwarzać niezbędne informacje zawierające dane osobowe.”,

c) uchyla się ust. 2;

4) po art. 52a dodaje się art. 52b–52d w brzmieniu:

„Art. 52b. 1. Przetwarzanie danych osobowych przez organy KAS w celu, o którym mowa w art. 1 ust. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na zasadach określonych w tej ustawie.

2. Administrator danych osobowych może przetwarzać dane osobowe zebrane pierwotnie w jednym z celów, o których mowa w art. 1 ust. 1 pkt 1 ustawy, o której mowa w ust. 1, do innych celów, o których mowa w art. 1 ust. 1 pkt 1 ustawy, o której mowa w ust. 1.

3. Dane, o których mowa w art. 15 ust. 1 ustawy, o której mowa w ust. 1, mogą być przetwarzane przez organy KAS wyłącznie, gdy jest to niezbędne ze względu na zakres lub charakter prowadzonego postępowania lub przeprowadzanych czynności lub na warunkach określonych w tym przepisie.

4. Danych osobowych, o których mowa w art. 15 ust. 1 ustawy, o której mowa w ust. 1, nie pobiera się w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej.

Art. 52c. 1. Dane osobowe zbierane i przetwarzane przez KAS na podstawie rozporządzenia 2016/679 mogą być przetwarzane przez organy KAS również dla celów określonych w art. 1 ust. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

2. Dane osobowe przetwarzane przez KAS dla celów określonych w art. 1 ust. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości mogą być przetwarzane przez organy KAS również dla innych celów.

Art. 52d. Organy KAS mogą przetwarzać dane osobowe bez wiedzy i zgody osób, których dane dotyczą.”;

5) w art. 124 dodaje się zdanie drugie w brzmieniu:

„Udostępnienie informacji zawierających dane osobowe odbywa się z zachowaniem przepisów ustawy z dnia …….. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.”;

6) 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, o których mowa w art. 113 ust. 1, odbywa się na zasadach określonych w ustawie z dnia …….. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, prawie Unii Europejskiej oraz postanowieniach umów międzynarodowych.”.

Art. 75. W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138 i 650) wprowadza się następujące zmiany:

1) w art. 51 skreśla się zdanie drugie.

2) w art. 56:

a) w ust. 6 pkt 1 otrzymuje brzmienie:

„1) dane osobowe, o których mowa w art. 15 ustawy z dnia …..… o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …);”,

b) w ust. 8 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Dane osobowe, o których mowa w ust. 2 i 3 oraz art. 40 ust. 1, z wyjątkiem danych osobowych, o których mowa w ust. 6 pkt 1, SOP może przetwarzać:”;

c) w ust. 9:

– w zdaniu pierwszym po wyrazie „SOP” dodaje się przecinek i wyrazy „z zastrzeżeniem ograniczeń określonych we właściwych przepisach o ochronie danych osobowych”,

– w zdaniu drugim wyrazy „5 lat” zastępuje się wyrazami „10 lat”,

d) skreśla się ust. 11;

3) w art. 59 ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„W celu realizacji zadań, o których mowa w art. 19 ust. 1 pkt 2, SOP może uzyskiwać dane:”;

4) art. 60 i 61 otrzymują brzmienie:

„Art. 60. Administratorem danych osobowych przetwarzanych przez SOP jest Komendant SOP.

Art. 61. Przetwarzanie danych osobowych przez SOP w celach, o którym mowa w art. 1 ust. 1 pkt 1 ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na zasadach określonych w tej ustawie.

2. Przetwarzanie danych osobowych przez SOP w celach innych niż wskazane w ust. 1, odbywa się na zasadach określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwanym dalej „rozporządzeniem (UE) 2016/679", z wyłączeniem przepisów art. 12–22 oraz art. 34 tego rozporządzenia.";

5) 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 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. 12–22 i art. 34 rozporządzenia (UE) 2016/679.

3. Administratorem danych osobowych, o których mowa w ust. 1, w zakresie w jakim przetwarza te dane, jest Komendant SOP.

4. Zasady i warunki przetwarzania informacji, w tym danych osobowych w celach, o których mowa w ust. 1, określa:

1) ustawa z dnia …….. o ochronie danych osobowych (Dz. U. poz. …);

2) rozporządzenie (UE) 2016/679 – z zastrzeżeniem, o którym mowa w ust. 2

5. Wyłączenia, o których mowa w ust. 2, stosuje się w przypadku informacji, w tym danych osobowych, niezbędnych do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień wynikających z ustawy.

6. Informacje, w tym dane osobowe, o których mowa w ust. 1, przetwarza się przez okres niezbędny do wykonania ustawowych zadań przez SOP. Administrator danych dokonuje weryfikacji tych danych nie rzadziej niż co 10 lat od dnia uzyskania informacji.".

Art. 76. W ustawie z dnia 10 stycznia 2018 r. o szczególnych rozwiązaniach związanych z organizacją w Rzeczypospolitej Polskiej sesji Konferencji Stron Ramowej konwencji

Narodów Zjednoczonych w sprawie zmian klimatu (Dz. U. poz. 319) wprowadza się następujące zmiany:

1) w art. 17:

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

„W celu zapewnienia bezpieczeństwa i porządku publicznego podczas Konferencji COP24, a także w celu zapobieżenia popełnianiu przestępstw i wykroczeń oraz wykrywania i ścigania ich sprawców, Policja i Służba Ochrony Państwa mogą przetwarzać informacje, w tym dane osobowe:”;

b) ust. 2 otrzymuje brzmienie;

„2. Do zakresu informacji, o których mowa w ust. 1, stosuje się odpowiednio przepisy art. 20 ust. 2b ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067 i 2405 oraz z 2018 r. poz. 106 i 138) oraz art. 56 ust. 6 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138 i 560).”

2) w art. 18:

a) ust. 1 otrzymuje brzmienie:

„1. Udostępnienie przez Policję oraz Służbę Ochrony Państwa informacji, o których mowa w art. 17 ust. 1, w celu zapewnienia bezpieczeństwa i porządku publicznego podczas Konferencji COP24, a także w celu zapobieżenia popełnianiu przestępstw i wykroczeń oraz wykrywania i ścigania ich sprawców, organom, służbom i instytucjom państwowym, w tym również odpowiednio zagranicznym i międzynarodowym, odbywa się na zasadach określonych odpowiednio w przepisach ustawy z dnia 6 kwietnia 1990 r. o Policji, ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, ustawy z dnia …… o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U….), ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167 i 1948 oraz z 2017 r. poz. 935), a także w umowach międzynarodowych, których Rzeczpospolita Polska jest stroną.”,

b) w ust. 2 zdanie pierwsze otrzymuje brzmienie:

„Policja i Służba Ochrony Państwa udostępniają informacje, o których mowa w art. 17 ust. 1 pkt 2, po uzyskaniu zgody organu, służby lub instytucji, które te informacje uzyskały lub przetwarzały.”,

c) w ust. 3 w pkt 1 otrzymuje brzmienie:

„1) udostępnianie tych informacji mogłoby utrudnić lub uniemożliwić realizację zadań Policji lub Służby Ochrony Państwa lub”;

3) w art. 19:

a) w ust. 1 po wyrazie „Policji” dodaje się wyrazy „lub Służby Ochrony Państwa”,

b) ust 2 otrzymuje brzmienie:

„2. Informacje, o których mowa w art. 17 ust. 1, usuwa się ze zbiorów danych osobowych, których administratorem jest Komendant Główny Policji lub Komendant Służby Ochrony Państwa, z wyjątkiem informacji, o których mowa odpowiednio w art. 20 ust. 2a ustawy z dnia 6 kwietnia 1990 r. o Policji i w art. 56 ust. 2 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, przetwarzanych na potrzeby toczących się postępowań, po upływie terminu, o którym mowa w art. 17 ust. 1.”;

4) w art. 20 po wyrazie „Policji” dodaje się przecinek i wyrazy „Służby Ochrony Państwa”.

Art. 77. W ustawie z dnia 26 stycznia 2018 r. o Straży Marszałkowskiej (Dz. U. poz…) wprowadza się następujące zmiany:

1) w art. 4:

a) po ust. 2 dodaje się ustęp 2a–2c w brzmieniu:

„2a. Przetwarzanie danych osobowych przez Straż Marszałkowską w celach, o którym mowa w art. 1 ust. 1 pkt 1 lit. d ustawy z dnia ..... o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. …), odbywa się na zasadach określonych w tej ustawie.

2b. Przetwarzanie danych osobowych przez Straż Marszałkowską w celach innych niż wskazane w ust. 2a, odbywa się na zasadach określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwanego dalej „rozporządzeniem (UE) 2016/679”, z wyłączeniem przepisów art. 12–22 oraz art. 34 tego rozporządzenia.

2c. Administratorem danych osobowych, o których mowa w ust. 1, w zakresie w jakim przetwarza te dane, jest Komendant Straży Marszałkowskiej.”,

b) w ust. 4 wyrazy „co 5 lat” zastępuje się wyrazami „co 10 lat”;

2) po art. 19 dodaje się art. 19a w brzmieniu:

„Art. 19a. 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 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. 12–22 i art. 34 rozporządzenia (UE) 2016/679.

3. Administratorem danych osobowych, o których mowa w ust. 1, w zakresie w jakim przetwarza te dane, jest Komendant Straży Marszałkowskiej.

4. Zasady i warunki przetwarzania informacji, w tym danych osobowych w celach, o których mowa w ust. 1, określa:

1) ustawa z dnia …… o ochronie danych osobowych (Dz. U. poz. …);

2) rozporządzenie (UE) 2016/679 – z zastrzeżeniem, o którym mowa w ust. 2

5. Wyłączenie, o którym mowa w ust. 2, stosuje się w przypadku informacji, w tym danych osobowych, niezbędnych do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień wynikających z ustawy.

6. Informacje, w tym dane osobowe, o których mowa w ust. 1, przetwarza się przez okres niezbędny do wykonania ustawowych zadań przez Straż Marszałkowską. Administrator danych dokonuje weryfikacji tych danych nie rzadziej niż co 10 lat od dnia uzyskania informacji.”.

Rozdział 10

Przepisy przejściowe, dostosowujące i końcowe

Art. 78. 1. Osoby wykonujące w dniu 6 maja 2018 r. funkcję administratora bezpieczeństwa informacji, o którym mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) pełnią funkcję inspektora ochrony danych nie dłużej jednak niż do dnia 1 września 2018 r.

2. W terminie, o którym mowa w ust. 1, administrator lub podmiot przetwarzający zawiadamiają organ nadzorczy, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady nr (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych

w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwanym dalej „rozporządzeniem 2016/679”, o wyznaczeniu inspektora ochrony danych, wskazując jego imię, nazwisko, adres poczty elektronicznej lub numer telefonu.

Art. 79. Do czynności kontrolnych wszczętych i nie zakończonych przed dniem 6 maja 2018 r. stosuje się:

1) do dnia wejścia w życie ustawy z dnia ……. o ochronie danych osobowych (Dz. U. poz. …) – przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
2) od dnia wejścia w życie ustawy z dnia ……. o ochronie danych osobowych – przepisy tej ustawy.

Art. 80. 1. Postępowania wszczęte i niezakończone prowadzone przed Generalnym Inspektorem Ochrony Danych Osobowych przed dniem wejścia w życie ustawy, toczą się przed Prezesem Urzędu Ochrony Danych Osobowych.

2. Postępowania, o których mowa w ust. 1, prowadzi się:

1) do dnia wejścia w życie ustawy z dnia ……. o ochronie danych osobowych – na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
2) od dnia wejścia w życie ustawy z dnia ……. o ochronie danych osobowych – na podstawie przepisów tej ustawy.

3. Wszystkie czynności przeprowadzone w postępowaniach, o których mowa w ust. 1, pozostają skuteczne.

4. W przypadku wniesienia zażalenia na postanowienie Generalnego Inspektora Ochrony Danych Osobowych, postępowanie wszczęte tym zażaleniem, umarza się z mocy prawa z dniem wejścia w życie ustawy z dnia …..… o ochronie danych osobowych.

5. Stronę, która zainicjowała postępowanie, o którym mowa w ust. 4, organ poucza o prawie zaskarżenia postanowienia wydanego przez Generalnego Inspektora Ochrony Danych Osobowych w skardze na decyzję Prezesa Urzędu Ochrony Danych Osobowych.

6. 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, postępowanie wszczęte tym wnioskiem umarza się z mocy prawa z dniem wejścia w życie ustawy z dnia …… o ochronie danych osobowych.

7. Stronę, która zainicjowała postępowanie, o których mowa w ust. 6, przed dniem wejścia w życie ustawy z dnia …… o ochronie danych osobowych, organ poucza o prawie złożenia skargi do sądu administracyjnego.

8. Termin na wniesienie skargi w przypadku, o którym mowa w ust. 6, 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.

9. Wszczęte i niezakończone przed dniem wejścia w życie ustawy postępowania prowadzone na podstawie rozdziału 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych umarza się z mocy prawa z dniem wejścia w życie ustawy z dnia …… o ochronie danych osobowych.

Art. 81. Podmiot, do którego przed dniem wejścia w życie ustawy, zostało skierowane wystąpienie lub wniosek, o których mowa w art. 19a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jest obowiązany przekazać Prezesowi Urzędu Ochrony Danych Osobowych odpowiedź na wystąpienie lub wniosek w terminie 30 dni od dnia wejścia w życie ustawy z dnia …… o ochronie danych osobowych.

Art. 82. W sprawach sądowych, sądowo-administracyjnych lub administracyjnych, wszczętych i nie zakończonych przed dniem wejścia w życie ustawy, w których stroną lub uczestnikiem był Generalny Inspektor Ochrony Danych Osobowych, stroną lub uczestnikiem staje się, z dniem wejścia w życie ustawy, Prezes Urzędu Ochrony Danych Osobowych.

Art. 83. 1. W terminie 1 roku od dnia wejścia w życie ustawy administrator dostosowuje zasady przetwarzania danych osobowych do środków technicznych i organizacyjnych, o których mowa w art. 39.

2. Jeżeli wymaga to niewspółmiernie dużego wysiłku administrator, może dostosować zautomatyzowane systemy przetwarzania danych osobowych do środków technicznych i organizacyjnych, w terminie dłuższym niż wskazanym w ust. 1, nie później jednak niż do dnia 6 maja 2023 r.

3. Dotychczasowe rozstrzygnięcia określające zasady udostępniania informacji i danych osobowych z Centralnej Bazy Danych Osób Pozbawionych Wolności, za pośrednictwem systemu teleinformatycznego, zachowują moc do dnia wejścia w życie decyzji wydanych na podstawie art. 25d ust. 1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, dodanego niniejszą ustawą, nie dłużej jednak niż do dnia 6 maja 2020 r.

4. Dostosowanie zasad przetwarzania informacji i danych osobowych w zbiorach danych utworzonych przed dniem 6 maja 2016 r. do wymogów, o których mowa w art. 20, art. 21 i art. 35, nastąpi w terminie 4 lat od dnia wejścia w życie niniejszej ustawy.

Art. 84. Wydane przed dniem wejścia w życie ustawy upoważnienia do przetwarzania danych osobowych zachowują moc przez okres 3 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 85. Zgody wydane przez służby, instytucje państwowe oraz organy władzy publicznej na udostępnianie za pomocą urządzeń telekomunikacyjnych lub w drodze teletransmisji informacji, w tym danych osobowych, jednostkom organizacyjnym Policji, jednostkom organizacyjnym Straży Granicznej lub Służbie Ochrony Państwa zachowują swoją moc.

Art. 86. W sprawach wszczętych i nie zakończonych przed dniem wejścia w życie niniejszej ustawy związanych z podejrzeniem popełnienia czynu zabronionego – w celach wyeliminowania pozostawionych przez nich śladów – Policja może pobrać odciski linii papilarnych lub wymazy ze śluzówki policzków od funkcjonariuszy i pracowników Policji wykonujących służbowe czynności związane z ujawnianiem, zabezpieczaniem lub badaniem śladów.

Art. 87. Karty daktyloskopijne wypełnione przed dniem wejścia w życie ustawy zachowują swoją moc.

Art. 88. Informatyczne nośniki danych wykorzystywane do przetwarzania danych osobowych po wycofaniu z eksploatacji przed dniem wejścia w życie niniejszej ustawy podlegają komisyjnemu zniszczeniu.

Art. 89. Do wyczerpania nakładów druków formularzy kart daktyloskopijnych, których wzory zostały określone na podstawie odrębnych przepisów, druki te mogą być stosowane, jednak nie dłużej niż do dnia 31 grudnia 2018 r.

Art. 90. Dotychczasowe przepisy wykonawcze wydane na podstawie:

1) art. 15 ust. 8, art. 20 ust. 19 oraz art. 20e ust. 4 ustawy zmienianej w art. 57,
2) art. 10a ust. 8 i art. 11 ust. 2 ustawy zmienianej w art. 58,
3) art. 25 ust. 3 ustawy zmienianej w art. 67,

4) art. 42 ust. 6 ustawy zmienianej w art. 68,

5) art. 24 ust. 5 ustawy zmienianej w art. 69

– zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie:

1) art. 15 ust. 8, art. 20 ust. 1q oraz art. 20e ust. 4 ustawy zmienianej w art. 57, w brzmieniu nadanym niniejszą ustawą,

2) art. 10a ust. 21 i art. 11 ust. 2 ustawy zmienianej w art. 58, w brzmieniu nadanym niniejszą ustawą,

3) art. 25 ust. 3 ustawy zmienianej w art. 67, w brzmieniu nadanym niniejszą ustawą,

4) art. art. 42 ust. 6 ustawy zmienianej w art. 68, w brzmieniu nadanym niniejszą ustawą,

5) art. 24a ust. 5 ustawy zmienianej w art. 69, w brzmieniu nadanym niniejszą ustawą

– nie dłużej jednak niż przez okres 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 91. 1. Maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy wynosi w roku:

1) 2018 r. – 700 000 zł;

2) 2019 r. – 1 100 000 zł;

3) 2020 r. – 1 200 000 zł;

4) 2021 r. – 1 200 000 zł;

5) 2022 r. – 1 300 000 zł;

6) 2023 r. – 1 300 000 zł;

7) 2024 r. – 1 300 000 zł;

8) 2025 r. – 1 300 000 zł;

9) 2026 r. – 1 400 000 zł;

10) 2027 r. – 1 400 000 zł;

11) 2028 r. – 1 400 000 zł.

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

3. W przypadku przekroczenia lub zagrożenia przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków określonego w ust. 1 oraz w przypadku, gdy w okresie od początku roku kalendarzowego do dnia ostatniej oceny, o której mowa w ust. 2, część limitu rocznego przypadającego proporcjonalnie na ten okres zostanie przekroczona co

najmniej o 10% stosuje się mechanizm korygujący polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym niniejszej ustawy.

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

Art. 92. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.