DODO
NAWIGATOR

USTAWA DODO

DYREKTYWA 2016/680

Tekst i praktyczne odesłania

Zawartość

Oddajemy w Państwa ręce treść ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (ustawa DODO) oraz powiązanej z nią 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.

Ze względu fakt, iż ustawa DODO miała implementować Dyrektywę 2016/680, przygotowaliśmy dla Państwa mapę praktycznych aspektów ustawy, które powiązaliśmy z odpowiadającymi im artykułami i motywami preambuły dyrektywy. Aby ułatwić nawigację, na marginesie samych przepisów wskazujemy: powiązane motywy z preambuły (P) oraz powiązane przepisy (D).

Mamy nadzieję, że przygotowana przez nas publikacja pozwoli na sprawniejsze przyswojenie treści przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz ułatwi zgodne z prawem, adekwatne i bezpieczne przetwarzanie danych osobowych przez Państwa organizację.

Patron opracowania

ODO 24 sp. z o. o. oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z zakresu m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

Autorzy opracowania

Piotr Liwszic - wieloletni pracownik instytucji państwowych, w których odpowiadał m.in. za nadzór nad bezpieczeństwem informacji, w tym informacji niejawnych. Prelegent na ogólnopolskich szkoleniach i konferencjach poświęconych bezpieczeństwu informacji. Brał udział w pracach legislacyjnych nad przepisami o ochronie informacji niejawnych. Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001). Współautor komentarza do ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Adw. dr Paweł Mielniczek – prawnik i naukowiec specjalizujący się w prawie międzynarodowym, ochronie praw jednostki i prawie nowych technologii. Doświadczenie zawodowe zdobywał m.in. w NATO, biurze ONZ w Genewie, dużej instytucji finansowej, biurze GIODO, UOKiK oraz kancelarii prawnej. Studiował na Uniwersytecie Warszawskim, the University of Manchester i the University of Florida. Posiada certyfikat Certified Information Privacy Manager (CIPM) Międzynarodowego Stowarzyszenia Specjalistów ds. Ochrony Prywatności (IAPP).

Tomasz Ochocki – ekspert ds. ochrony danych. Kierownik zespołu merytorycznego ODO 24. Doświadczenie zawodowe zdobywał zarówno w państwowych instytucjach centralnych, jak i w sektorze prywatnym. Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001), systemu zarządzania ciągłością działania (ISO 22301) oraz audytor wewnętrzny systemu zarządzania prywatnością (ISO/IEC 27701). Posiada aktualny certyfikat metodyki zarządzania projektami PRINCE2. Współautor komentarza do ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Adw. Łukasz Pociecha – ekspert ds. ochrony danych. Do jego kompetencji należy kompleksowa obsługa klientów w zakresie ochrony danych osobowych i bezpieczeństwa informacji, w tym m.in.: sporządzenie opinii prawnych i umów oraz przeprowadzanie audytów. Prelegent licznych szkoleń poświęconych ochronie danych osobowych i bezpieczeństwu informacji. Posiada aktualny certyfikat metodyki zarządzania projektami PRINCE2. Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001). Współautor komentarza do ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Ilustracja na okładce: Karol Banach (www.karolbanach.com)

Projekt, skład i wersja elektroniczna: Wojciech Rataj

ISBN: 78-83-943435-4-5

Warszawa, sierpień 2020 r.

Spis treści

Mapa praktycznych aspektów

Administrator

- Ustawa DODO: art. 4 pkt 1, art. 31, art. 32, art. 39-43
- Dyrektywa 2016/680: art. 3, 4, 10, 19, 20, 23, 29, 63
- preambuła dyrektywy: motywy 11, 21-24, 26, 29, 30, 37, 47, 50-53, 55, 60

Ewidencjonowanie czynności przetwarzania

- Ustawa DODO: art. 36
- Dyrektywa 2016/680: art. 25
- preambuła dyrektywy: motywy 57, 96

Informowanie o naruszeniach ochrony danych

- Ustawa DODO: art. 44, 45
- Dyrektywa 2016/680: art. 30, 31, 39
- preambuła dyrektywy: motywy 61, 62

Inspektor ochrony danych

- Ustawa DODO: art. 46, 47
- Dyrektywa 2016/680: art. 27, 32-34
- preambuła dyrektywy: motyw 63

Ocena skutków planowanych operacji przetwarzania

- Ustawa DODO: art. 37, 38
- Dyrektywa 2016/680: art. 27, 28, 34
- preambuła dyrektywy: motywy 51, 52, 53, 58, 59, 60

Organ nadzorczy

- Ustawa DODO: art. 5-10,
- Ustawa o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781): art. 34
- Dyrektywa 2016/680: art. 46, 50
- preambuła dyrektywy: motywy 77, 83

Podmiot przetwarzający (procesor)

- Ustawa DODO: art. 4 pkt 12, art. 34
- Dyrektywa 2016/680: art. 4, 22, 29
- preambuła dyrektywy: motywy 54-56, 60

Podstawy prawne przetwarzania

- Ustawa DODO: art. 13-14
- Dyrektywa 2016/680: art. 4, 8, 9, 10
- preambuła dyrektywy: motywy 26, 33, 35, 37

Prawa osoby, której dane dotyczą

- Ustawa DODO: art. 22-30
- Dyrektywa 2016/680: art. 3, 12, 13, 14, 15, 17-19, 29, 30, 52
- preambuła dyrektywy: motywy 20, 39, 40-49, 50, 52

Privacy by design & by default

- Ustawa DODO: art. 32
- Dyrektywa 2016/680: art. 20
- preambuła dyrektywy: motywy 53, 55

Profilowanie

- Ustawa DODO: art. 4 pkt 13, art. 15, art. 35
- Dyrektywa 2016/680: art. 3, 11
- preambuła dyrektywy: motyw 38

Przekazywanie danych osobowych innym organom, państwu trzeciemu i organizacji międzynarodowej

- Ustawa DODO: art. 21
- Dyrektywa 2016/680: art. 35-40
- preambuła dyrektywy: motywy 32, 34-39, 64-72, 74

Pseudonimizacja

- Ustawa DODO: art. 4 pkt 15, art. 32
- Dyrektywa 2016/680: art. 3 pkt 5, art. 20
- preambuła dyrektywy: motywy 51, 53, 61

Rozróżnienie danych osobowych

- Ustawa DODO: art. 19, 20
- Dyrektywa 2016/680: art. 4, 6, 7
- preambuła dyrektywy: motywy 31

Zabezpieczenie danych na podstawie oszacowanego ryzyka

- Ustawa DODO: art. 31, 32, 39
- Dyrektywa 2016/680: art. 4, 10, 19, 20, 29, 63
- preambuła dyrektywy: motywy 23, 26, 29, 37, 50, 52, 53, 55, 60

Weryfikacja danych osobowych

- Ustawa DODO: art. 16
- Dyrektywa 2016/680: art. 4, 5, 11
- preambuła dyrektywy: motywy 26, 30, 32, 41

Współadministratorzy

- Ustawa DODO: art. 33
- Dyrektywa 2016/680: art. 21
- preambuła dyrektywy: motyw 54

Wykaz kategorii czynności przetwarzania

- Ustawa DODO: art. 35
- Dyrektywa 2016/680: art. 21, 24
- preambuła dyrektywy: motywy 50, 56

Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125)

Rozdział I. Przepisy ogólne (art. 1–4).

D: 1, 2, 9
P: 4, 5, 7

Artykuł 1. Zakres przedmiotowy.

Ustawa określa:

1) zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności;
2) prawa osób, których dane osobowe są przetwarzane przez właściwe organy w celach, o których mowa w pkt 1, oraz środki ochrony prawnej przysługujące tym osobom;
3) sposób prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez właściwe organy w celach, o których mowa w pkt 1, z wyłączeniem danych osobowych przetwarzanych przez prokuraturę i sądy;
4) zadania organu nadzorczego oraz formy i sposób ich wykonania;

5) obowiązki administratora i podmiotu przetwarzającego oraz inspektora ochrony danych i tryb jego wyznaczania;
6) sposób zabezpieczenia danych osobowych;
7) tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej;
8) odpowiedzialność karną za naruszenie przepisów niniejszej ustawy.

D: 2, 3
P: 17, 18, 21, 34

Artykuł 2. Stosowanie ustawy.

Ustawę stosuje się do przetwarzania danych osobowych przez właściwe organy w celach, o których mowa w art. 1 pkt 1, w sposób:
1) całkowicie lub częściowo zautomatyzowany;
2) inny niż zautomatyzowany, w przypadku gdy dane te stanowią lub mają stanowić część zbioru danych.

D: 2
P: 10-12, 14

Artykuł 3. Wyłączenie stosowania.

Przepisów ustawy nie stosuje się do ochrony danych osobowych:
1) znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz.U. z 2018 r. poz. 969), ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz.U. z 2018 r. poz. 652, 1010, 1387 i 2432), ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 2018 r. poz. 1987 i 2399), ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz.U. z 2018 r. poz. 1958, 2192, 2193, 2227 i 2354), ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. z 2018 r. poz. 475, z późn. zm.), ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub

wolności seksualnej innych osób (Dz.U. z 2014 r. poz. 24, z 2015 r. poz. 396, z 2016 r. poz. 2205 oraz z 2018 r. poz. 2435), ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz.U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5, 1000, 1443 i 1669);

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

D: 3
P: 11, 21-24, 30, 47, 51, 53

Artykuł 4. Objaśnienie pojęć.

Ilekroć w ustawie jest mowa o:

1) administratorze – rozumie się przez to właściwy organ, który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych, podmiot wskazany przez ustawę jako administrator, jeżeli cele i sposoby przetwarzania danych osobowych są określone w ustawie, albo podmiot wskazany przez prawo Unii Europejskiej albo prawo państwa członkowskiego Unii Europejskiej lub podmiot wyznaczony zgodnie z kryteriami określonymi w prawie tego państwa;
2) danych biometrycznych – rozumie się przez to dane osobowe dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, w tym wizerunek twarzy lub dane daktyloskopijne, które zostały uzyskane wskutek specjalnego przetwarzania technicznego;
3) danych dotyczących zdrowia – rozumie się przez to dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym dane o korzystaniu z usług opieki zdrowotnej, które ujawniają informacje o stanie jej zdrowia;

4) danych genetycznych – rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które zostały uzyskane w szczególności z analizy próbki biologicznej pochodzącej od tej osoby;
5) danych osobowych – rozumie się przez to dane osobowe, o których mowa w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.);
6) naruszeniu ochrony danych osobowych – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
7) odbiorcy – rozumie się przez to osobę fizyczną lub prawną, organ władzy publicznej, jednostkę organizacyjną lub inny podmiot, któremu ujawnia się dane osobowe, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego Unii Europejskiej, a przetwarzanie tych danych jest zgodne z przepisami o ochronie danych mającymi zastosowanie do ich celów przetwarzania;
8) ograniczeniu przetwarzania – rozumie się przez to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
9) organie nadzorczym w innych państwach Unii Europejskiej – rozumie się przez to niezależny organ publiczny ustanowiony przez inne niż Rzeczpospolita Polska państwo członkowskie Unii

Europejskiej, powołany dla ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej;

10) organizacji międzynarodowej – rozumie się przez to organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;
11) państwie trzecim – rozumie się przez to państwo niebędące państwem członkowskim Unii Europejskiej i niestosujące przepisów dorobku Schengen;
12) podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ władzy publicznej, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
13) profilowaniu – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na ich wykorzystaniu do oceny niektórych cech osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
14) przetwarzaniu – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
15) pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, aby nie można ich było już przypi-

sać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

16) właściwym organie – rozumie się przez to organ władzy publicznej, jednostkę organizacyjną lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych;
17) zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rozdział 2. Zadania organu nadzorczego.

D: 41, 46
P: 77

Artykuł 5. Zakres zadań Prezesa Urzędu Ochrony Danych Osobowych.

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

1) monitorowanie i egzekwowanie stosowania przepisów niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych;
2) upowszechnianie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych w celu, o którym mowa w art. 1 pkt 1;
3) doradzanie instytucjom publicznym w sprawach środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych w celu, o którym mowa w art. 1 pkt 1;
4) upowszechnianie wiedzy z zakresu stosowania niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych wśród administratorów i podmiotów przetwarzających;

5) udzielanie osobie, której dane dotyczą, na jej żądanie, informacji o wykonywaniu praw przysługujących jej na mocy niniejszej ustawy, a w miarę potrzeby współpracowanie w tym celu z organami nadzorczymi w innych państwach Unii Europejskiej;
6) rozpatrywanie skarg osób, których dane osobowe są przetwarzane niezgodnie z prawem, i prowadzenie postępowań w tym zakresie;
7) o ile przepis szczególny nie stanowi inaczej, kontrola zgodności przetwarzania danych osobowych z przepisami niniejszej ustawy;
8) prowadzenie postępowania w sprawie stosowania niniejszej ustawy, w tym na podstawie informacji otrzymanych od innego organu władzy publicznej;
9) pełnienie funkcji konsultacyjnych, o których mowa w art. 38, dotyczących operacji przetwarzania w ramach niniejszej ustawy;
10) współpraca z organami nadzorczymi w innych państwach członkowskich Unii Europejskiej;
11) wydawanie opinii dla Sejmu, Senatu oraz innych organów władzy publicznej w sprawach ochrony danych osobowych;
12) wydawanie opinii w odniesieniu do projektów ustaw i rozporządzeń w sprawach dotyczących ochrony danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1.

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

3. Projekty ustaw i rozporządzeń dotyczące danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1, są przedstawiane do zaopiniowania Prezesowi Urzędu.

D: 41, 46
P: 81

Artykuł 6. Kontrola przetwarzania danych osobowych.

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

D: 47

Artykuł 7. Zakres uprawnień kontrolującego.

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

D: 3, 30, 41, 42, 43, 47
P: 77, 81, 82

Artykuł 8. Ostrzeżenie, nakaz przywrócenia stanu zgodnego z prawem.

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

2. W przypadku naruszenia przepisów o ochronie danych osobowych zbieranych w celach, o których mowa w art. 1 pkt 1, Prezes

Urzędu, w drodze decyzji administracyjnej, nakazuje administratorowi lub podmiotowi przetwarzającemu przywrócenie stanu zgodnego z prawem, a w szczególności:

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

3. Decyzje Prezesa Urzędu, o których mowa w ust. 2, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Administrator w przypadku uznania, że zgromadzone w ten sposób dane są zbędne, jest obowiązany do ich usunięcia. W przypadku niedopełnienia obowiązku usunięcia danych osobowych przez administratora Prezes Urzędu może nakazać ich usunięcie. W celu realizacji uprawnienia Prezes Urzędu nie uzyskuje dostępu do danych osobowych, o których mowa w zdaniu pierwszym. Administrator lub podmiot przetwarzający dane osobowe, o których mowa w zdaniu pierwszym, jest obowiązany do niezwłocznego przywrócenia zgodnego z prawem sposobu ich przetwarzania.

Artykuł 9. Jednoinstancyjność postępowania.

D: 47, 53

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

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

D: 47
P: 82

Artykuł 10. Wystąpienia Prezesa Urzędu.

1. W celu realizacji zadań, o których mowa w art. 5 ust. 1 pkt 5 i 9, Prezes Urzędu może kierować do administratora lub podmiotu przetwarzającego wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych zbieranych w celach, o których mowa w art. 1 pkt 1.

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

D: 34, 47

Artykuł 11. Przeprowadzenie przez inspektora ochrony danych sprawdzenia.

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

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

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

Artykuł 12. Odesłanie do KPA.

D: 53

Do postępowań w sprawach objętych zakresem regulacji niniejszego rozdziału stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2018 r. poz. 2096 oraz z 2019 r. poz. 60), zwanej dalej "Kodeksem postępowania administracyjnego", o ile przepisy niniejszej ustawy nie stanowią inaczej.

Rozdział 3. Zasady dotyczące przetwarzania danych osobowych.

Artykuł 13. Zakres przetwarzania danych osobowych.

D: 4, 8, 9
P: 26, 33, 35

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

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

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

3. Dopuszcza się przetwarzanie danych osobowych w innych celach niż określone w art. 1 pkt 1, jeżeli przepisy prawa zezwalają na ich przetwarzanie.

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

D: 4, 8, 9, 10
P: 26, 35, 37

Artykuł 14. Zakres przetwarzania danych wrażliwych.

1. Niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej, zwanych dalej ”danymi wrażliwymi”.

2. Dopuszcza się przetwarzanie danych wrażliwych, jeżeli:

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

D: 3, 11
P: 38

Artykuł 15. Niedopuszczalność profilowania osób fizycznych.

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

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

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

D: 4, 5, 11
P: 26, 30, 32, 41

Artykuł 16. Weryfikacja danych osobowych.

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

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

D: 4, 5
P: 41

Artykuł 17. Przekształcenie danych osobowych uznanych za zbędne.

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

D: 4, 5, 8
P: 33

Artykuł 18. Pozostawienie danych po ich zanonimizowaniu.

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

D: 4, 6
P: 31

Artykuł 19. Rozróżnianie danych przez administratora.

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

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

D: 4, 7
P: 31

Artykuł 20. Rozróżnianie na dane osobowe mające źródło w faktach i w indywidualnych ocenach.

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

D: 7, 8, 35-40
P: 32, 34-39, 64-72, 74

Artykuł 21. Warunki przesyłania lub udostępniania danych osobowych innym organom, państwu trzeciemu lub organizacji międzynarodowej.

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

2. Właściwy organ, przesyłając dane osobowe odbiorcy, o którym mowa w ust. 1, przekazuje, w miarę potrzeby i możliwości, nie-

zbędne dodatkowe informacje pozwalające temu odbiorcy ocenić stopień prawidłowości, kompletności oraz aktualności przesłanych danych osobowych.

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

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

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

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

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

6. Jeżeli przepisy prawa zezwalają szczególne warunki przetwarzania, właściwy organ przesyłający jest obowiązany do poinformowania odbiorcy takich danych osobowych o tych warunkach i obowiązku ich przestrzegania.

Rozdział 4. Prawa osoby, której dane dotyczą.

D: 12, 13, 14, 15, 17, 52
P: 39, 40, 42, 43

Artykuł 22. Zakres danych udostępnianych przez administratora.

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

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

3. Osobie, której dane dotyczą, w konkretnych przypadkach w celu umożliwienia wykonywania przysługujących jej praw, administrator przekazuje co najmniej następujące informacje:
1) podstawa prawna przetwarzania;
2) okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
3) odbiorcy lub kategorii odbiorców, którym dane osobowe zostały ujawnione, w szczególności odbiorcy w państwach trzecich lub organizacjach międzynarodowych.

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

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

D: 14, 15, 17, 30
P: 43-46, 48, 52

Artykuł 23. Prawo dostępu do danych osobowych na wniosek.

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

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

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

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

D: 16, 17, 52
P: 47, 48

Artykuł 24. Wniosek o sprostowanie lub usunięcie danych.

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

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

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

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

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

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

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

Artykuł 25. Obowiązek czasowego ograniczenia przetwarzania kwestionowanych danych.

D: 16, 52
P: 47, 48

1. Jeżeli:

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

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

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

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

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

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

D: 13, 15, 19, 29
P: 20, 44, 49

Artykuł 26. Zakaz udostępniania danych w razie zagrożenia życia lub zdrowia.

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

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

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

D: 3, 18
P: 20

Artykuł 27. Dane osobowe zgromadzone w postępowaniach prowadzonych na podstawie ustaw.

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

Artykuł 28. Zakres danych wymaganych we wniosku.

D: 12
P: 41

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

Artykuł 29. Pouczenie o możliwości wniesienia skargi do Prezesa Urzędu.

D: 15, 52

Administrator w przypadku, o którym mowa w art. 26 ust. 1, poucza osobę, której dane dotyczą, o możliwości wniesienia skargi do Prezesa Urzędu w sposób określony w art. 30 ust. 2.

Artykuł 30. Komunikacja prowadzona przez administratora z osobą zainteresowaną.

D: 12, 13
P: 40, 50

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

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

3. Administrator, bez zbędnej zwłoki, informuje pisemnie w postaci papierowej lub elektronicznej lub za pośrednictwem środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

(Dz.U. z 2019 r. poz. 123) osobę, której dane dotyczą, o działaniach podjętych w związku z jej wnioskiem lub, jeżeli to możliwe, udziela wnioskowanych informacji.

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

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

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

6. Administrator bez zbędnej zwłoki, lecz nie później niż w terminie do 14 dni od dnia złożenia wniosku, o którym mowa w art. 22 ust. 4, art. 23 ust. 1 lub art. 24 ust. 1, powiadomi wnioskodawcę o wysokości opłaty, o której mowa w ust. 4 pkt 1. Udzielenie informacji zgodnie z wnioskiem następuje w terminie do 14 dni od uiszczenia opłaty, chyba że wnioskodawca dokona w tym terminie zmiany wniosku co do zakresu żądanych danych, sposobu lub formy ich udostępnienia albo wycofa wniosek.

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

Rozdział 5. Administrator i podmiot przetwarzający.

Oddział 1. Przepisy ogólne.

D: 4, 10, 19, 29
P: 23, 26, 29, 37

Artykuł 31. Obowiązki administratora.

1. Administrator zapewnia, aby dane osobowe były:

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

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

3. Administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych i prawidłową realiza-

cję czynności w tym zakresie, o których mowa w ust. 1 i 2 i art. 13–21, oraz jest obowiązany do prowadzenia dokumentacji dotyczącej realizacji tych czynności. Dopuszcza się prowadzenie tej dokumentacji w postaci elektronicznej.

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

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

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

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

D: 19, 20, 29
P: 50, 52, 53, 55, 60

Artykuł 32. Środki techniczne i organizacyjne stosowane przez administratora.

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

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

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

D: 21
P: 54

Artykuł 33. Współadministratorzy.

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

2. Współadministratorzy:

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

   – chyba że przepisy prawa, którym ci administratorzy podlegają, określają przypadające im obowiązki i ich zakres;
2) wyznaczają punkt kontaktowy dla osób, których dane dotyczą, w celu realizacji obowiązku, o którym mowa w pkt 1 lit. a.

D: 4, 22, 29
P: 54-56, 60

Artykuł 34. Podmiot przetwarzający.

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

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

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

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

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

b) usunąć wszelkie istniejące kopie danych osobowych – chyba że przepisy prawa wymagają przechowywania danych osobowych;

6) udostępniać administratorowi wszelkie informacje związane z weryfikacją prawidłowości realizacji umowy powierzenia, o której mowa w ust. 1;

7) przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, któremu powierzył przetwarzanie danych osobowych.

6. Podmiot przetwarzający może powierzyć przetwarzanie danych innemu podmiotowi przetwarzającemu każdorazowo wyłącznie na podstawie pisemnej umowy, w przypadku gdy umowa, o której mowa w ust. 1, przewiduje takie prawo, na warunkach i w zakresie przez nią określonym.

7. W przypadkach powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze, co nie wyłącza odpowiedzialności podmiotu przetwarzającego za przetwarzanie danych niezgodnie z ustawą lub umową, o której mowa w ust. 1.

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

Artykuł 35. Wykaz kategorii czynności przetwarzania.

D: 21, 24
P: 50, 56

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

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

1) imię i nazwisko lub nazwę oraz dane kontaktowe:
   a) administratora,

b) współadministratora – w przypadku, o którym mowa w art. 33 ust. 1,
c) inspektora ochrony danych,
d) podmiotu przetwarzającego – w przypadku, o którym mowa w art. 34 ust. 2 i 6;
2) cele przetwarzania;
3) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
4) opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych;
5) informacje o stosowaniu profilowania – w przypadku gdy zostało ono zastosowane;
6) kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
7) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;
8) planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe;
9) ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych, o których mowa w art. 39, jeżeli jest to możliwe.

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

4. W wykazie, o którym mowa w ust. 3, zamieszcza się następujące informacje:
1) imię i nazwisko lub nazwę oraz dane kontaktowe:
a) podmiotu przetwarzającego w przypadku, o którym mowa w art. 34 ust. 2 i 6,
b) każdego administratora, w imieniu którego działa podmiot przetwarzający,
c) inspektora ochrony danych;

2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
3) przypadki przekazania danych osobowych do państw trzecich lub organizacji międzynarodowej, w razie jednoznacznego polecenia administratora, łącznie z nazwą tego państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpiło;
4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 39, w miarę możliwości.

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

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

D: 25
P: 57, 96

Artykuł 36. Ewidencjonowanie operacji przetwarzania.

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

2. Ewidencjonowaniu podlegają operacje przetwarzania, w szczególności:
1) zbieranie;
2) modyfikowanie;
3) przeglądanie;
4) ujawnianie wraz z przekazywaniem;
5) łączenie;
6) usuwanie.

3. Ewidencja jest prowadzona automatycznie, w sposób pozwalający ustalić zasadność operacji w oparciu o informacje wskazujące:
1) datę i godzinę operacji;
2) tożsamość osoby, która przeglądała lub ujawniła dane osobowe – w miarę możliwości;
3) tożsamość odbiorców danych osobowych – w miarę możliwości.

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

5. Ewidencje obejmujące czynności przetwarzania są przeznaczone wyłącznie:
1) do weryfikacji zgodności przetwarzania z prawem;
2) do monitorowania własnej działalności;
3) dla zapewnienia integralności i bezpieczeństwa danych osobowych;
4) na potrzeby postępowania karnego.

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

D: 27, 28
P: 50, 51, 53, 58, 60

Artykuł 37. Ocena skutków planowanych operacji przetwarzania.

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

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

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

D: 24, 28, 34
P: 59

Artykuł 38. Wniosek o konsultacje.

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

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

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

3. Administrator przedstawia Prezesowi Urzędu:

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

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

mowa w ust. 1, przedstawia administratorowi lub podmiotowi przetwarzającemu pisemne zalecenia.

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

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

Oddział 2. Zabezpieczenie danych osobowych.

D: 19, 29, 63
P: 50, 52, 53, 60

Artykuł 39. Środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

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).

Artykuł 40. Nośniki wycofane z eksploatacji, niszczenie danych.

D: 29, 63

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

D: 23

Artykuł 41. Wniosek o nadanie uprawnień dostępu do danych osobowych.

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

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

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

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

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

D: 23, 29
P: 50

Artykuł 42. Ewidencja osób upoważnionych do przetwarzania danych osobowych.

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

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

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

Artykuł 43. Obowiązek zapewnienia bezpieczeństwa danych osobowych.

D: 23, 29

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

Artykuł 44. Zgłoszenie naruszenia ochrony Prezesowi Urzędu.

D: 30
P: 61, 62

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

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

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

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

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

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

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

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

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

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

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

Artykuł 45. Zawiadomienie o naruszeniu ochrony danych osobowych.

D: 31, 39
P: 61, 62

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

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

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, jeżeli został spełniony jeden z poniższych warunków:
1) administrator zastosował odpowiednie techniczne i organizacyjne środki ochrony, w szczególności szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wskazanych w ust. 1;
3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku.

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

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

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

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

Oddział 3. Inspektor ochrony danych.

D: 32-34
P: 63

Artykuł 46. Wymagania wobec inspektora ochrony danych.

1. Administrator wyznacza inspektora ochrony danych.

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

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

4. Administrator, który wyznaczył inspektora, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności, z uwzględnieniem kryteriów, o których mowa w ust. 2.

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

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

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

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

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

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

11. Administrator udostępnia dane inspektora ochrony danych, o których mowa w ust. 9, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Artykuł 47. Zadania inspektora ochrony danych.

D: 27, 32-34
P: 63

1. Do zadań inspektora ochrony danych należy:

1) informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy

niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;
2) prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania;
3) monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami niniejszej ustawy oraz innymi przepisami dotyczącymi ochrony danych;
4) monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem;
5) współpraca z Prezesem Urzędu;
6) monitorowanie realizacji zaleceń, o których mowa w art. 38 ust. 4, oraz przedstawianie Prezesowi Urzędu stanu ich realizacji;
7) pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 38, oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach;
8) pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących jej praw, o których mowa w rozdziale 4;
9) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37, oraz monitorowanie wykonania tych zaleceń;
10) sporządzanie i przekazywanie administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

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

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

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

Rozdział 6. Współpraca z organami nadzorczymi w innych państwach Unii Europejskiej.

Artykuł 48. Wniosek o pomoc.

D: 46, 50
P: 77, 83

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

2. Wniosek o pomoc dotyczy w szczególności:
1) udzielenia informacji;
2) przeprowadzenia:
   a) konsultacji,
   b) kontroli,
   c) postępowań.

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

4. Prezes Urzędu może odmówić realizacji wniosku o pomoc wyłącznie w przypadku, gdy:
1) nie jest organem właściwym w zakresie przedmiotu tego wniosku;
2) wykonanie tego wniosku naruszyłoby przepis prawa.

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

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

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

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

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

D: 46, 50
P: 77, 83

Artykuł 49. Zakres wniosku o pomoc.

1. Prezes Urzędu może występować do organu nadzorczego w innych państwach Unii Europejskiej z wnioskiem o pomoc, w szczególności o udzielenie informacji, przeprowadzenie konsultacji, kontroli lub postępowań.

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

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

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

Rozdział 7. Środki ochrony prawnej i odpowiedzialność prawna.

Artykuł 50. Prawo wniesienia skargi do Prezesa Urzędu na naruszenia.

D: 45, 52
P: 48, 80, 85

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

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

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

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

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

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

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

D: 53
P: 85, 86

Artykuł 51. Prawo do wniesienia skargi do sądu administracyjnego.

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

2. Każdej osobie, której dane dotyczą, przysługuje prawo do wniesienia do sądu administracyjnego skargi, jeżeli Prezes Urzędu nie rozpatrzył skargi lub zgłoszenia wniesionego na mocy art. 50 lub nie poinformował osoby, której dane dotyczą, w terminie 3 miesięcy od dnia wpływu skargi, o postępach lub wyniku jej rozpatrzenia.

3. Do rozpatrywania skarg stosuje się przepisy ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2018 r. poz. 1302, 1467, 1544 i 1629 oraz z 2019 r. poz. 11 i 60), z tym że:

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

Artykuł 52. Umocowanie organizacji społecznej o charakterze niezarobkowym do reprezentowania osoby.

D: 55
P: 87

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.

Artykuł 53. Prawo do odszkodowania lub zadośćuczynienia.

D: 54, 56
P: 88

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

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

3. W sprawach o stwierdzenie niezgodności działania administratora z przepisami niniejszej ustawy, Prezes Urzędu może wytoczyć powództwo na rzecz i w imieniu osoby, o której mowa w ust. 1, a także wstąpić do postępowania przed sądem w każdym jego stadium.

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

Rozdział 8. Przepisy karne.

D: 57
P: 89

Artykuł 54. Niedopuszczalność przetwarzania danych.

1. Kto przetwarza dane osobowe, o których mowa w przepisach o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

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

D: 57

Artykuł 55. Utrudnianie przeprowadzania kontroli.

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

Rozdział 9. Zmiany w przepisach.

Artykuł 56. Zmiany w ustawie o Trybunale Stanu.

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

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

Art. 20g. 1. Nadzór nad przetwarzaniem danych osobowych przez Trybunał Stanu w ramach prowadzonych przez niego postępowań wykonuje Krajowa Rada Sądownictwa.
2. Do nadzoru, o którym mowa w ust. 1, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz.U. z 2019 r. poz. 52, 55, 60 i 125) stosuje się odpowiednio.".

Artykuł 57. Zmiany w ustawie o rybactwie śródlądowym.

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

1) po art. 22 dodaje się art. 22a i art. 22b w brzmieniu:
„Art. 22a. 1. Państwowa Straż Rybacka w celu realizacji ustawowych zadań jest uprawniona do przetwarzania informacji, w tym danych osobowych, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzania danych genetycznych lub danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej.
2. Państwowa Straż Rybacka może przetwarzać dane osobowe bez wiedzy i zgody osoby, której dane dotyczą, w celu realizacji swoich ustawowych zadań.
3. Administratorem danych osobowych przetwarzanych w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), jest komendant wojewódzki Państwowej Straży Rybackiej.
4. Państwowa Straż Rybacka w celu realizacji zadań ustawowych, w szczególności dotyczących wykrywania i zwalczania prze-

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

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

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

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

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

Art. 22b. 1. Państwowa Straż Rybacka jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w Państwowej Straży Rybackiej, przenoszenia do służby w Państwowej Straży Rybackiej oraz w zakresie wynikającym z przebiegu stosunku służbowego funkcjonariuszy Państwowej Straży Rybackiej, także po jego ustaniu, w tym ma prawo prze-

twarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia (UE) 2016/679, z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie pracowników posiadających pisemne upoważnienie wydane przez administratora danych oraz pisemnym zobowiązaniu pracowników do zachowania przetwarzanych danych w poufności."

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

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

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

3. Administratorem danych osobowych przetwarzanych w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jest komendant właściwej jednostki Społecznej Straży Rybackiej."

Artykuł 58. Zmiany w ustawie o Policji.

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

1) w art. 1 w ust. 2 pkt 8 otrzymuje brzmienie:
   „8) przetwarzanie informacji kryminalnych, w tym danych osobowych;";
2) w art. 5b w ust. 1 po wyrazach"w zakresie zleconym przez Inspektora Nadzoru Wewnętrznego – funkcjonariuszy i pracowników" dodaje się wyraz"Policji,";
3) w art. 14:
   a) w ust. 1 w pkt 1 po wyrazie"przestępstw" dodaje się przecinek i wyrazy"przestępstw skarbowych",
   b) w ust. 4 wyrazy"ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922)" zastępuje się wyrazami"ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125)";
4) w art. 15:
   a) w ust. 1:
      – w pkt 3a w lit. c średnik zastępuje się przecinkiem i dodaje się lit. d w brzmieniu:
         „d) w celu identyfikacji lub wykrywania sprawców przestępstw – na zasadach określonych w niniejszej ustawie;",
      – po pkt 5a dodaje się pkt 5b w brzmieniu:
      „5b) obserwowania i rejestrowania przy użyciu środków technicznych obrazu lub dźwięku w trakcie interwencji w miejscach innych niż publiczne, podczas prowadzenia działań kontrterrorystycznych oraz wspierania działań jednostek organizacyjnych Policji przez służbę kontrterrorystyczną w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił

i środków oraz specjalistycznej taktyki działań, a także w policyjnych środkach transportu;",

b) po ust. 7b dodaje się ust. 7c w brzmieniu:
„7c. Użyte w ust. 1 pkt 5b określenie interwencja oznacza włączenie się policjanta lub policjantów w tok zdarzenia mogącego naruszać normy prawne i podjęcie działań zmierzających do ustalenia charakteru, rodzaju i okoliczności powstałego zdarzenia oraz przedsięwzięć ukierunkowanych na przywrócenie naruszonego porządku prawnego."

c) ust. 8 otrzymuje brzmienie:
„8. Rada Ministrów określi, w drodze rozporządzenia, sposób postępowania przy wykonywaniu uprawnień, o których mowa w ust. 1 pkt 1, 2a, 3, pkt 3a lit. b–d, pkt 3b, 5a–7, 9 i 10, wzory dokumentów stosowanych w tych sprawach oraz w odniesieniu do ust. 1 pkt 5b również sposób przechowywania, odtwarzania i kopiowania zapisów obrazu i dźwięku, mając na względzie zapewnienie skuteczności działań podejmowanych przez Policję, poszanowanie praw osób, wobec których działania te są podejmowane oraz konieczność właściwego zabezpieczenia utrwalonego obrazu i dźwięku przed utratą, zniekształceniem, a także zapewnienie ochrony praw osób, których wizerunek został utrwalony."

5) po art. 15a dodaje się art. 15b i art. 15c w brzmieniu:
„Art. 15b. Informacje uzyskane podczas realizacji czynności, o których mowa w art. 15 ust. 1 pkt 5a i 5b, w tym dane osobowe niezawierające dowodów pozwalających na wszczęcie postępowania karnego albo postępowania w sprawach o wykroczenia, postępowania dyscyplinarnego lub mogących być wykorzystanymi w postępowaniu w ramach czynności wyjaśniających albo dowodów mających znaczenie dla toczących się takich postępowań, Policja przechowuje przez okres co najmniej 30 dni, nie dłużej jednak niż 60 dni od dnia zarejestrowania, a następnie je niszczy. W przypadku czynności operacyjno-rozpoznawczych

terminy, o których mowa w zdaniu pierwszym, są liczone od dnia zakończenia realizacji tych czynności.

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

6) w art. 20:
   a) ust. 1 otrzymuje brzmienie:
      „1. W celu realizacji zadań ustawowych Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, z zachowaniem ograniczeń wynikających z art. 19."
   b) po ust. 1 dodaje się ust. 1a–1o w brzmieniu:
      1a. Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może dotyczyć danych osobowych, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przy czym dane dotyczące wyników analizy kwasu deoksyrybonukleinowego (DNA) obejmują informacje wyłącznie o niekodującej części DNA.
      1b. Uzyskiwanie informacji, w tym danych osobowych, może odbywać się z wykorzystaniem środków technicznych.
      1c. Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do realizacji zadań ustawowych lub wykonywania uprawnień związanych z prowadzeniem postępowań administracyjnych, realizacją czynności administracyjno-porządkowych oraz innych czynności, do przeprowadzania których funkcjonariusze Policji są uprawnieni na podstawie ustaw, w celach innych niż określone w art. 1 pkt 1 ustawy z dnia 14 grud-

nia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem (UE) 2016/679", z wyłączeniem danych dotyczących kodu genetycznego.

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

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

w tym prowadzonej kontroli operacyjnej.

1e. Podmioty, o których mowa w ust. 1d, mogą wyrazić pisemną zgodę na udostępnianie danych zgromadzonych w zbiorach danych jednostkom organizacyjnym Policji w drodze teletransmisji, bez konieczności składania wnio-

sku pisemnie w postaci papierowej lub elektronicznej, jeżeli jednostki te spełniają łącznie następujące warunki:

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

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

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

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

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

1j. Przetwarzanie danych osobowych przez Policję w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na podstawie ustawy, prawa Unii Europejskiej oraz postanowień umów międzynarodowych.
1k. W przypadku podejrzanych Policja pobiera wymazy ze śluzówki policzków oraz dane osobowe, o których mowa w art. 21a ust. 2 pkt 2 lit. b–h i art. 21h ust. 2 pkt 2 i 3, w celach, o których mowa w art. 15 ust. 1 pkt 3a lit. d.
1l. Policja pobiera odciski linii papilarnych lub wymazy ze śluzówki policzków od funkcjonariuszy i pracowników Policji wykonujących służbowe czynności związane z ujawnianiem, zabezpieczaniem lub badaniem śladów związanych z podejrzeniem popełnienia czynu zabronionego w celach wyeliminowania pozostawionych przez nich śladów.
1m. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb pobierania odcisków linii papilarnych lub wymazów ze śluzówki policzków od funkcjonariuszy i pracowników Policji oraz sposób przeprowadzania i dokumentowania czynności związanych z ich pobieraniem, a także rodzaje służb policyjnych uprawnionych do korzystania ze zbiorów danych zawierających odciski linii papilarnych lub wymazy ze śluzówki policzków od funkcjonariuszy i pracowników Policji oraz sposób zabezpieczenia tych zbiorów uniemożliwiający identyfikację funkcjonariusza lub pracownika Policji, których dane dotyczą, przez osobę nieupoważnioną, uwzględniając konieczność wyeliminowania pozostawionych przez nich śladów.
1n. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wzory dokumentów obowiązujących przy przetwarzaniu danych, uwzględniając potrzebę ochrony danych przed nieuprawnionym dostępem i prze-

słanki zaniechania zbierania określonych rodzajów informacji, a w przypadku wymiany informacji – uwzględniając konieczność dostosowania się do wymogów określonych przez organy innych państw, zobowiązania międzynarodowe Rzeczypospolitej Polskiej lub przez Międzynarodową Organizację Policji Kryminalnej – Interpol.

1o. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wzory kart daktyloskopijnych, na których dane daktyloskopijne są pobierane przez upoważnione podmioty i przekazywane Komendantowi Głównemu Policji w celu przetwarzania w zbiorach danych daktyloskopijnych, oraz tryb i sposób ich przekazywania Komendantowi Głównemu Policji przez obowiązane do tego służby, instytucje państwowe oraz organy władzy publicznej – uwzględniając charakter realizowanych zadań i celów przeznaczenia danej karty daktyloskopijnej.

c) uchyla się ust. 2a,

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

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

2ab. Policja jest uprawniona do przetwarzania i wymiany informacji, w tym danych osobowych osób ubiegających się o przyjęcie do pracy w agencjach Unii Europejskiej zajmujących się zapobieganiem lub zwalczaniem czynów zabronionych, międzynarodowych organach sądowniczych, międzynarodowych organach ścigania oraz w Międzynarodowej Organizacji Policji Kryminalnej – Interpol, za zgodą tych

osób. Policja, przekazując wyniki przetwarzania, zastrzega, że nie udostępnia się ich osobie, której dane osobowe dotyczą.

e) uchyla się ust. 2ac,

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

„1) dane osobowe, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z tym że dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA;”,

g) ust. 2c otrzymuje brzmienie:

2c. Danych osobowych, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej.

h) w ust. 4 dodaje się zdanie trzecie w brzmieniu:

„Informacje i dane udostępnia się także organom ścigania państw członkowskich Unii Europejskiej, agencjom Unii Europejskiej zajmującym się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol, jeżeli następuje to w celu ścigania karnego.”,

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

j) uchyla się ust. 15–19;

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

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

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

a) w ust. 1 we wprowadzeniu do wyliczenia po wyrazie”przestępstw” dodaje się przecinek i wyrazy”przestępstw skarbowych”,
b) po ust. 6 dodaje się ust. 6a w brzmieniu:
„6a. Komendant Główny Policji, Komendant CBŚP, Komendant BSWP albo komendant wojewódzki (Stołeczny) Policji może upoważnić swojego zastępcę do realizacji czynności, o których mowa w ust. 6.”
c) dodaje się ust. 8 w brzmieniu:
„8. Dane, o których mowa w ust. 1, pobiera się i udostępnia się także organom ścigania państw członkowskich Unii Europejskiej i innych państw, agencjom Unii Europejskiej zajmującymi się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol na ich wniosek, jeżeli następuje to w celu wykrywania przestępstw oraz ścigania ich sprawców, ratowania życia lub zdrowia ludzkiego albo poszukiwania osób zaginionych.”

9) w art. 20cb:
a) w ust. 1 we wprowadzeniu do wyliczenia po wyrazie”przestępstw” dodaje się przecinek i wyrazy”przestępstw skarbowych”,
b) ust. 2 otrzymuje brzmienie:
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, przepisy art. 20c ust. 2–8 stosuje się.
10) w art. 20da w ust. 1 wyrazy”przepisy art. 20c ust. 2–7 stosuje się” zastępuje się wyrazami”przepisy art. 20c ust. 2–8 stosuje się”;
11) w art. 20e ust. 1 otrzymuje brzmienie:
1. Komendant Główny Policji prowadzi System Wspomagania Dowodzenia Policji, zwany dalej”SWD Policji”, będący systemem teleinformatycznym wspierającym:
1) wykonywanie zadań ustawowych przez jednostki organizacyjne Policji;

2) obsługę zgłoszeń alarmowych, o których mowa w ustawie z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz.U. z 2018 r. poz. 867 i 1115).

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

13) dodaje się art. 20g w brzmieniu:

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

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

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

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

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

14) art. 21a–21e otrzymują brzmienie:
„Art. 21a. 1. Komendant Główny Policji prowadzi zbiór danych zawierający informacje o wynikach analizy kwasu deoksyrybonukleinowego (DNA), zwany dalej”zbiorem danych DNA”, którego jest administratorem w rozumieniu ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
2. W zbiorze danych DNA przetwarza się:
1) informacje, w tym dane osobowe, o których mowa w ust. 1, w odniesieniu do:
a) osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego,
b) nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego,
c) osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz.U. z 2014 r. poz. 24, z 2015 r. poz. 396, z 2016 r. poz. 2205 oraz z 2018 r. poz. 2435),
d) osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2018 r. poz. 452, 650 i 730),
e) oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego,
f) osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość,
g) zwłok ludzkich o nieustalonej tożsamości,
h) śladów nieznanych sprawców przestępstw,
i) osób zaginionych,
j) osób, o których mowa w art. 15 ust. 1 pkt 3a lit. c,
k) osób, o których mowa w art. 20 ust. 1l;

2) informacje, w tym dane osobowe osób, o których mowa w pkt 1 lit. a–e oraz i–k, obejmują:
   a) wyniki analizy kwasu deoksyrybonukleinowego (DNA),
   b) imiona, nazwiska lub pseudonimy,
   c) imiona i nazwiska rodowe rodziców tych osób,
   d) datę i miejsce urodzenia,
   e) adres zamieszkania,
   f) numer PESEL,
   g) obywatelstwo i płeć,
   h) oznaczenie i cechy dokumentu tożsamości.

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

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

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

ludzkich o nieustalonej tożsamości, osób zaginionych oraz osób, o których mowa w art. 15 ust. 1 pkt 3a lit. c.

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

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

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

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

Art. 21e. 1. W weryfikacji, o której mowa w art. 16 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku zapobieganiem i zwalczaniem przestępczości, uczestniczą jednostki organizacyjne Policji, służby, instytucje państwowe lub organy władzy publicznej, które przekazały informacje, w tym dane osobowe, do zbioru danych DNA.

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

1) zostało umorzone postępowanie z uwagi na to, że:
   a) czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia,

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

2) osoba, której dane dotyczą:
   a) została uniewinniona prawomocnym wyrokiem sądu,
   b) ukończyła 100. rok życia,
   c) zmarła;
3) tożsamość zwłok ludzkich została ustalona;
4) utracą swoją przydatność eliminacyjną, jednakże nie dłużej niż po upływie 5 lat od dnia ustania stosunku służbowego lub pracy – w przypadku osób, o których mowa w art. 20 ust. 1l.

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

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

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

15) uchyla się art. 21f i art. 21g;
16) art. 21h–21n otrzymują brzmienie:
„Art. 21h. 1. Komendant Główny Policji prowadzi następujące zbiory danych daktyloskopijnych, których jest administratorem w rozumieniu przepisów o ochronie danych osobowych:

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

– zwane dalej"zbiorami danych daktyloskopijnych".

2. W zbiorach danych daktyloskopijnych są przetwarzane:

1) informacje, w tym dane osobowe, dotyczące:
   a) osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego,
   b) nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego,
   c) osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób,
   d) osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych,
   e) oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego,
   f) osób poszukiwanych,
   g) cudzoziemców, od których zostały pobrane odciski linii papilarnych w sytuacjach, o których mowa w art. 35 ust. 2, art. 324 pkt 1 i art. 394 ust. 3 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach lub art. 30 ust. 1 pkt 3, art. 92 ust. 1 i art. 114 ust. 1 ustawy z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej, lub art. 73a

ustawy z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin (Dz.U. z 2017 r. poz. 900 oraz z 2018 r. poz. 650),

h) śladów linii papilarnych, które mogą pochodzić od osób zaginionych,
i) niezidentyfikowanych śladów linii papilarnych z miejsc przestępstw,
j) osób, o których mowa w art. 20 ust. 1l;

2) informacje, w tym dane osobowe, przetwarzane w zbiorze danych, o którym mowa w ust. 1 pkt 1, obejmują:
   a) imiona, nazwiska lub pseudonimy,
   b) imiona i nazwiska rodowe rodziców tych osób,
   c) datę i miejsce urodzenia,
   d) oznaczenie i cechy identyfikacyjne dokumentu tożsamości,
   e) adres zamieszkania,
   f) numer PESEL,
   g) obywatelstwo i płeć,
   h) oznaczenie i numer sprawy,
   i) miejsce i powód daktyloskopowania,
   j) odciski linii papilarnych palców i dłoni;
3) informacje, w tym dane osobowe, przetwarzane w zbiorze danych, o którym mowa w ust. 1 pkt 2, obejmujące:
   a) obrazy odcisków linii papilarnych,
   b) rok urodzenia,
   c) płeć,
   d) rodzaj rejestracji,
   e) datę wprowadzenia,
   f) jednostkę organizacyjną wprowadzającą;
4) informacje, w tym dane osobowe, dotyczące niezidentyfikowanych śladów linii papilarnych z miejsc przestępstw obejmujące:

a) obrazy śladów linii papilarnych,
b) datę i miejsce zabezpieczenia,
c) kategorię przestępstwa,
d) jednostkę organizacyjną wprowadzającą,
e) oznaczenie i numer sprawy;

5) informacje, w tym dane osobowe, dotyczące śladów linii papilarnych, które mogą pochodzić od osób zaginionych, obejmujące:
a) obrazy śladów linii papilarnych,
b) datę i miejsce zabezpieczenia,
c) kategorię zdarzenia,
d) jednostkę organizacyjną wprowadzającą,
e) oznaczenie i numer sprawy.

3. W zbiorach danych daktyloskopijnych przetwarza się, z wyłączeniem przechowywania, informacje, w tym dane osobowe, dotyczące osób o nieustalonej tożsamości lub usiłujących ukryć swoją tożsamość oraz zwłok ludzkich o nieustalonej tożsamości, obejmujące:
1) obrazy odcisków linii papilarnych;
2) płeć;
3) oznaczenie i numer sprawy.

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

Art. 21j. Informacje, w tym dane osobowe, przetwarzane w zbiorach danych daktyloskopijnych oraz uzyskane w wyniku ich przetwarzania są udzielane bezpłatnie organom prowadzącym:
1) postępowanie karne;
2) postępowanie w sprawach nieletnich;
3) czynności wykrywcze lub identyfikacyjne;
4) czynności związane z wprowadzaniem danych daktyloskopijnych do innych zbiorów danych na podstawie odrębnych przepisów.

Art. 21k. 1. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. a–h, są przechowywane w zbiorach danych daktyloskopijnych w celu prowadzenia czynności identyfikacyjnych.
2. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. a–f, są przechowywane w zbiorach danych daktyloskopijnych i wykorzystywane w celu prowadzenia czynności wykrywczych.
3. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. j, są przetwarzane w zbiorach danych daktyloskopijnych w celu wyeliminowania, spośród wszystkich zebranych w toku prowadzonego postępowania, śladów pozostawionych przez osoby, o których mowa w art. 20 ust. 1l.
Art. 21l. 1. W weryfikacji, o której mowa w art. 16 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, uczestniczą jednostki organizacyjne Policji, służby, instytucje państwowe lub organy władzy publicznej, które przekazały informacje, w tym dane osobowe, do zbiorów danych daktyloskopijnych.
2. Informacje, w tym dane osobowe, o których mowa w art. 21h ust. 2 pkt 1 lit. a–c, e i f, usuwa się ze zbiorów danych daktyloskopijnych, w przypadku gdy:
1) zostało umorzone postępowanie z uwagi na to, że:
   a) czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia,
   b) zdarzenie lub okoliczność, w związku z którymi wprowadzono dane osobowe do zbioru danych, nie ma znamion czynu zabronionego;
2) osoba, której dane dotyczą:
   a) została uniewinniona prawomocnym wyrokiem sądu,
   b) ukończyła 100. rok życia,

c) zmarła;

3) utracą swoją przydatność eliminacyjną, jednakże nie dłużej niż po upływie 5 lat od dnia ustania stosunku służbowego lub pracy – w przypadku osób, o których mowa w art. 20 ust. 1o.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia (UE) 2016/679, w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie policjantów lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowiązaniu policjantów lub pracowników do zachowania przetwarzanych danych w poufności.

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

19) w art. 145j:

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

„7) krajowego punktu dostępu do systemu Eurodac, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniającym rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona) (Dz.Urz. UE L 180 z 29.06.2013, str. 1), zwanym dalej ”rozporządzeniem (UE) 603/2013”.”,

c) 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."

d) 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."

Artykuł 59. Zmiany w ustawie o Straży Granicznej.

W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz.U. z 2017 r. poz. 2365, z późn. zm.[8)]) 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 mię-

dzynarodowymi, w tym z Międzynarodową Organizacją Policji Kryminalnej – Interpol.

2) w art. 3c w ust. 1 po wyrazach ”w zakresie zleconym przez Inspektora Nadzoru Wewnętrznego – funkcjonariuszy i pracowników Policji” dodaje się wyrazy ”, Straży Granicznej,”;

3) w art. 9:

a) ust. 1 otrzymuje brzmienie:

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

b) w ust. 1a wyrazy „ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922)” zastępuje się wyrazami „ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125)”;

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

„Art. 9ca. 1. Straż Graniczna w celu ochrony obiektów, o których mowa w art. 9c ust. 1, może wprowadzić nadzór nad terenem użytkowanych obiektów lub terenem przyległym do obiektów w postaci środków technicznych oraz urządzeń elektronicznego systemu monitorującego stan bezpieczeństwa obiektu umożliwiających rejestrację obrazu, a także środków organizacyjnych i technicznych zapewniających

identyfikację i kontrolę osób przebywających w użytkowanych obiektach, w tym przepustek zawierających wizerunek twarzy, oraz systemów teleinformatycznych przetwarzających informacje o przepustkach, w tym dane osób, którym je wydano.

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

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

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

5) art. 10a otrzymuje brzmienie:

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

2. Straż Graniczna przetwarza dane osobowe w zakresie niezbędnym do realizacji ustawowych zadań lub wykonywania uprawnień związanych z zapobieganiem i zwalczaniem przestępstw oraz przestępstw skarbowych, a także wykroczeń oraz wykroczeń skarbowych, w tym dane osobowe, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych

w związku z zapobieganiem i zwalczaniem przestępczości, przy czym dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA.

3. Danych osobowych, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej.

4. Straż Graniczna przetwarza dane osobowe w zakresie niezbędnym do realizacji ustawowych zadań lub wykonywania uprawnień związanych z prowadzeniem postępowań administracyjnych, dokonywaniem kontroli granicznej, realizacją czynności administracyjno-porządkowych oraz innych kontroli albo czynności, do prowadzenia których funkcjonariusze Straży Granicznej są uprawnieni na podstawie ustaw, w tym mają prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.), zwanego dalej ”rozporządzeniem (UE) nr 2016/679”, z wyłączaniem danych dotyczących kodu genetycznego.

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

1) wymazy ze śluzówki policzków oraz imiona, nazwiska lub pseudonimy, imiona i nazwiska rodowe rodziców tych osób, datę i miejsce urodzenia, adres zamieszkania, numer PESEL, obywatelstwo i płeć;
2) odciski linii papilarnych palców i dłoni oraz imiona, nazwiska lub pseudonimy, imiona i nazwiska rodowe

rodziców tych osób, datę i miejsce urodzenia, oznaczenie i cechy identyfikacyjne dokumentu tożsamości, adres zamieszkania, numer PESEL, obywatelstwo i płeć, oznaczenie i numer sprawy, miejsce i powód daktyloskopowania, obrazy odcisków linii papilarnych, rodzaj rejestracji, datę rejestracji.

6. Przetwarzanie danych osobowych przez Straż Graniczną w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na podstawie ustawy, prawa Unii Europejskiej oraz postanowień umów międzynarodowych.

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

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

1) gromadzonych w administrowanych przez nich zbiorach danych lub rejestrach;

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

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

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

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

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

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

13. Komendant Główny Straży Granicznej może upoważnić osoby, o których mowa w ust. 12, do udzielania i cofania, w jego imieniu, upoważnień do przetwarzania danych oso-

bowych, o których mowa w ust. 11, podległym im pracownikom i funkcjonariuszom Straży Granicznej.
14. Wyłączenia wynikające z przepisów o ochronie danych osobowych nie naruszają prawa osoby do ubiegania się o informacje jej dotyczące, w formie podania o zaświadczenie, jeżeli osoba wykaże interes prawny w urzędowym potwierdzeniu określonych faktów lub stanu prawnego.
15. Straż Graniczna udostępnia właściwym podmiotom informacje, o których mowa w art. 1 ust. 2 pkt 9, w tym dane osobowe, na wniosek przekazany pisemnie w postaci papierowej lub elektronicznej, który powinien zawierać podstawę prawną, przeznaczenie oraz wskazanie, w zależności od rodzaju informacji, jakie mają zostać udostępnione, przedziału czasowego podlegającego sprawdzeniu, danych osoby, pojazdu, dokumentu podlegających sprawdzeniu, a także podpis upoważnionej osoby.
16. Przepisu ust. 15 nie stosuje się do udostępniania informacji, w tym danych osobowych, podmiotom występującym o ich przekazanie w związku z wykonywaniem przez te podmioty czynności operacyjno-rozpoznawczych lub prowadzeniem postępowań przygotowawczych.
17. Udostępnianie informacji, o których mowa w art. 1 ust. 2 pkt 9, w tym danych osobowych, może nastąpić w drodze teletransmisji, bez konieczności składania pisemnego wniosku, jeżeli odrębne przepisy dotyczące zadań i uprawnień podmiotów, o których mowa w art. 1 ust. 2 pkt 9, przewidują taką możliwość, podmioty spełniają określone w tych przepisach warunki, a Komendant Główny Straży Granicznej wyrazi pisemną zgodę w postaci papierowej lub elektronicznej na taki sposób udostępnienia informacji, w tym danych osobowych.
18. Minister właściwy do spraw wewnętrznych w porozumieniu z Ministrem Sprawiedliwości określi, w drodze rozporządzenia, sposób pobierania wymazów ze śluzówki policzków,

gromadzenia odcisków linii papilarnych oraz zdjęć sygnalitycznych osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, osób o nieustalonej tożsamości lub osób usiłujących ukryć swoją tożsamość, warunki przechowywania, wykorzystania i sposób ich przekazywania innym organom uprawnionym na podstawie przepisów odrębnych, a także wzory wykorzystywanych dokumentów, uwzględniając przypadki i sposoby pobierania odcisków linii papilarnych, przeprowadzania wywiadu daktyloskopijnego oraz wykonywania zdjęć sygnalitycznych, a także kierując się potrzebą ochrony tych danych przed nieuprawnionym dostępem.

6) w art. 10b:
   a) w ust. 1 po wyrazie ”przestępstw” dodaje się wyrazy ”oraz przestępstw skarbowych”,
   b) dodaje się ust. 8 w brzmieniu:
      „8. Dane, o których mowa w ust. 1, pobiera się i udostępnia się także organom ścigania państw członkowskich Unii Europejskiej i innych państw, agencjom Unii Europejskiej zajmującym się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol na ich wniosek, jeżeli następuje to w celu wykrywania przestępstw oraz ścigania ich sprawców albo w celu ratowania życia i zdrowia ludzkiego.”
7) w art. 10bb:
   a) w ust. 1 po wyrazie ”przestępstw” dodaje się wyrazy ”oraz przestępstw skarbowych”,
   b) ust. 2 otrzymuje brzmienie:
      2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, przepisy art. 10b ust. 2–8 stosuje się.
8) w art. 11:
   a) w ust. 1:
      – po pkt 5b dodaje się pkt 5c–5e w brzmieniu:

„5c) pobierania od osób odcisków linii papilarnych lub wymazu ze śluzówki policzków:
a) w trybie i przypadkach określonych w przepisach Kodeksu postępowania karnego,
b) w celu identyfikacji osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość, jeżeli ustalenie tożsamości w inny sposób nie jest możliwe;
5d) pobierania od cudzoziemców odcisków linii papilarnych w trybie i przypadkach określonych w przepisach odrębnych;
5e) utrwalania wizerunku osób w celu weryfikacji ich tożsamości, identyfikacji osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość;",

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

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

c) ust. 2 otrzymuje brzmienie:

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

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

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

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

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

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

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

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

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

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy Straży Granicznej lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowią-

zaniu funkcjonariuszy Straży Granicznej lub pracowników do zachowania przetwarzanych danych w poufności.

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

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

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

Artykuł 60. Zmiany w ustawie o obszarach morskich RP i administracji morskiej.

W ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz.U. z 2018 r. poz. 2214) po art. 43a dodaje się art. 43b w brzmieniu:

„Art. 43b. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), jest dyrektor urzędu morskiego.”.

Artykuł 61. Zmiany w ustawie o Inspekcji Ochrony Środowiska.

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

5. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), jest minister właściwy do spraw środowiska, Główny Inspektor Ochrony Środowiska lub wojewódzki inspektor ochrony środowiska.

Artykuł 62. Zmiany w ustawie o lasach.

W ustawie z dnia 28 września 1991 r. o lasach (Dz.U. z 2018 r. poz. 2129 i 2161 oraz z 2019 r. poz. 83) w art. 47 po ust. 2b dodaje się ust. 2c w brzmieniu:

2c. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), jest minister właściwy do spraw środowiska lub Główny Inspektor Straży Leśnej.

Artykuł 63. Zmiany w ustawie Prawo łowieckie.

W ustawie z dnia 13 października 1995 r. – Prawo łowieckie (Dz.U. z 2018 r. poz. 2033) w art. 39 po ust. 2 dodaje się ust. 2a w brzmieniu:

2a. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r.

poz. 125), jest minister właściwy do spraw środowiska lub komendant wojewódzki Państwowej Straży Łowieckiej.

Artykuł 64. Zmiany w ustawie o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych.

W ustawie z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (Dz.U. z 2018 r. poz. 2216 oraz z 2019 r. poz. 15) w art. 11t uchyla się ust. 9.

Artykuł 65. Zmiany w ustawie Prawo energetyczne.

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

„8) Policji – jeżeli jest to konieczne do skutecznego zapobieżenia popełnieniu przestępstwa, jego wykrycia albo ustalenia sprawców i uzyskania dowodów, na zasadach i w trybie określonych w art. 20 ust. 1d i 1e ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2017 r. poz. 2067, z późn. zm.[11]);".

Artykuł 66. Zmiany w ustawie Kodeks karny wykonawczy.

W ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz.U. z 2018 r. poz. 652, 1010, 1387 i 2432) wprowadza się następujące zmiany:

1) w art. 11 § 1a otrzymuje brzmienie:
„§ 1a. Jeżeli pokrzywdzony złożył wniosek, o którym mowa w art. 168a § 1, sąd, o którym mowa w § 1, przesyła dyrektorowi zakładu karnego lub aresztu śledczego ten wniosek oraz dane zawierające imię, nazwisko i adres pokrzywdzonego. W wypad-

ku, 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.".

Artykuł 67. Zmiany w ustawie Prawo o ustroju sądów wojskowych.

W ustawie z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych (Dz.U. z 2018 r. poz. 1921) po art. 6a dodaje się art. 6b i art. 6c w brzmieniu:

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

§ 2. Do przetwarzania danych osobowych w postępowaniach sądowych przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej "rozporządzeniem 2016/679", nie stosuje się.

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

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

1) w zakresie działalności wojskowego sądu garnizonowego – prezes wojskowego sądu okręgowego;
2) w zakresie działalności wojskowego sądu okręgowego – Krajowa Rada Sądownictwa.

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

Artykuł 68. Zmiany w ustawie o strażach gminnych.

W ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. z 2018 r. poz. 928 i 2399) dotychczasową treść art. 10a oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

2. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), przez straż jest komendant straży.

Artykuł 69. Zmiany w ustawie o żegludze śródlądowej.

W ustawie z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz.U. z 2017 r. poz. 2128 oraz z 2018 r. poz. 1137 i 1694) w art. 10 po ust. 5 dodaje się ust. 5a w brzmieniu:

5a. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), jest dyrektor urzędu żeglugi śródlądowej.

Artykuł 70. Zmiany w ustawie o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych.

W ustawie z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (Dz.U. z 2019 r. poz. 44) wprowadza się następujące zmiany:

1) tytuł ustawy otrzymuje brzmienie: ”o przetwarzaniu informacji kryminalnych”
2) art. 1 i art. 2 otrzymują brzmienie:
   „Art. 1. Ustawa określa zasady postępowania przy przetwarzaniu informacji kryminalnych w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania i zwalczania przestępczości, a także podmioty właściwe w tych sprawach.
   Art. 2. 1. Na zasadach określonych w niniejszej ustawie informacje kryminalne przetwarza się w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania i zwalczania przestępczości.
   2. Informacje kryminalne przetwarza się bez wiedzy i zgody osoby, której dane dotyczą, oraz z zachowaniem zasad ich ochrony określonych w przepisach o ochronie informacji niejawnych.
   3. Informacje kryminalne przekazuje się podmiotom uprawnionym, o których mowa w art. 19, w innych celach niż określone w ust. 1, w zakresie niezbędnym dla realizacji ich zadań ustawowych, w szczególności w celu ochrony bezpieczeństwa i porządku publicznego, zapobiegania i zwalczania zdarzeń oraz zagrożeń o charakterze terrorystycznym lub prowadzenia działań kontrterrorystycznych, jeżeli podmioty te są uprawnione na pod-

stawie ustawy do przetwarzania informacji, w tym danych osobowych, wchodzących w zakres informacji kryminalnych w celu realizacji określonego zadania.

3) w art. 4 pkt 4 otrzymuje brzmienie:
   „4) przetwarzanie informacji kryminalnych – oznacza przetwarzanie w rozumieniu art. 4 pkt 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125);";
3) w art. 5:
   a) ust. 1 otrzymuje brzmienie:
      1. Organem administracji rządowej właściwym w sprawach przetwarzania i przekazywania informacji kryminalnych jest Komendant Główny Policji.
   b) po ust. 1 dodaje się ust. 1a w brzmieniu:
      1a. Komendant Główny Policji jest administratorem danych osobowych, przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
4) w art. 6:
   a) pkt 1 otrzymuje brzmienie:
      „1) przetwarzanie i przekazywanie informacji kryminalnych;",
   b) pkt 4 otrzymuje brzmienie:
      „4) zapewnienie bezpieczeństwa przetwarzanym w Centrum informacjom kryminalnym, zgodnie z przepisami ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r. poz. 412, 650, 1000, 1083 i 1669).";

5) w art. 13 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:
„Zakres przetwarzanych informacji kryminalnych obejmuje następujące dane:"
6) w art. 16 ust. 1 otrzymuje brzmienie:
1. W bazach danych gromadzi się informacje kryminalne otrzymane od podmiotów zobowiązanych, o których mowa w art. 20, przekazane w odpowiedzi na zapytanie lub z własnej inicjatywy.

8) w art. 18 wprowadza się następujące zmiany:
a) uchyla się ust. 1,
b) ust. 2 otrzymuje brzmienie:
2. W zakresie nieuregulowanym w niniejszej ustawie do przetwarzania i przekazywania informacji kryminalnych stosuje się przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

9) tytuł rozdziału 4 otrzymuje brzmienie:
„Przetwarzanie i analiza informacji kryminalnych"

11) w art. 29 ust. 2 otrzymuje brzmienie:
2. Na wniosek organu Policji, o którym mowa w art. 5b ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2017 r. poz. 2067, z późn. zm.[13)]), zwanej dalej "ustawą o Policji", lub organu Straży Granicznej, o którym mowa w art. 3c ust. 2 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz.U. z 2017 r. poz. 2365, z późn. zm.[14)]), zwanej dalej "ustawą o Straży Granicznej", w przypadku udostępnienia informacji kryminalnej w zakresie realizacji zadań ustawowych określonych w art. 5b ust. 1 ustawy o Policji lub art. 3c ust. 1 ustawy o Straży Granicznej przepisu ust. 1 nie stosuje się.

11) w art. 33 w ust. 1 po pkt 2 dodaje się przecinek i pkt 3 w brzmieniu:
„3) realizacja zadań ustawowych w zakresie ochrony bezpieczeństwa i porządku publicznego, zapobieganie i zwalczanie

zdarzeń oraz zagrożeń o charakterze terrorystycznym lub prowadzenie działań kontrterrorystycznych".

Artykuł 71. Zmiany w ustawie Prawo o ustroju sądów powszechnych.

W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz.U. z 2019 r. poz. 52, 55 i 60) wprowadza się następujące zmiany:

1) w art. 175a w § 1:
   a) wprowadzenie do wyliczenia otrzymuje brzmienie: „Administratorami danych osobowych:"
   b) pkt 2 otrzymuje brzmienie:
      „2) referendarzy sądowych, asystentów sędziów, dyrektorów sądów oraz ich zastępców, kuratorów sądowych, aplikantów aplikacji sądowej, aplikantów kuratorskich, urzędników oraz innych pracowników sądów,",
   c) część wspólna wyliczenia otrzymuje brzmienie:
      „są prezesi i dyrektorzy właściwych sądów oraz Minister Sprawiedliwości, w zakresie realizowanych zadań."
2) po art. 175d dodaje się art. 175da–175dd w brzmieniu:
   „Art. 175da. Administratorami danych osobowych przetwarzanych w systemach teleinformatycznych obsługujących postępowania sądowe, w systemach teleinformatycznych, w których są prowadzone rejestry sądowe, oraz w systemach teleinformatycznych, w których są prowadzone urządzenia ewidencyjne (sądowe systemy teleinformatyczne), są sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej, prezesi właściwych sądów oraz Minister Sprawiedliwości w ramach realizowanych zadań.
   Art. 175db. Administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania

wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej są sądy.

Art. 175dc. § 1. Do przetwarzania danych osobowych w postępowaniach sądowych, w rejestrach sądowych albo w sądowych systemach teleinformatycznych nie stosuje się przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[15)]), zwanego dalej "rozporządzeniem 2016/679".

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

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

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

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

1) rozpatrują skargi osób, których dane osobowe są przetwarzane niezgodnie z prawem;
2) podejmują działania mające na celu upowszechnianie wśród nadzorowanych administratorów i podmiotów przetwarzających wiedzy o obowiązkach wynikających z rozporządzenia 2016/679 oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych

w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125);

3) współpracują z innymi organami sprawującymi nadzór nad przetwarzaniem danych osobowych w ramach postępowań prowadzonych przez sądy i trybunały oraz z organami nadzorczymi w rozumieniu art. 51 rozporządzenia 2016/679, w tym dzielą się informacjami oraz świadczą wzajemną pomoc, w celu zapewnienia spójnego stosowania rozporządzenia 2016/679 oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

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

1) nakazywania administratorowi lub podmiotowi przetwarzającemu albo ich przedstawicielom dostarczenia wszelkich informacji potrzebnych do realizacji zadań tego organu;
2) zawiadamiania administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
3) uzyskiwania od administratora i podmiotu przetwarzającego dostępu do danych osobowych i informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;
4) uzyskiwania dostępu do pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych;
5) wydawania ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
6) udzielania upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów roz-

porządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;

7) wzywania administratora lub podmiotu przetwarzającego do dostosowania przetwarzania danych do przepisów rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

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

Artykuł 72. Zmiany w ustawie o Żandarmerii Wojskowej i wojskowych organach porządkowych.

W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2018 r. poz. 430, 650, 1544 i 2399 oraz z 2019 r. poz. 53) wprowadza się następujące zmiany:

1) w art. 4 w ust. 2 w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu:
„19) przetwarzanie informacji, w tym danych osobowych.”;

2) art. 29 otrzymuje brzmienie:
„Art. 29. 1. Żandarmeria Wojskowa w celu realizacji ustawowych zadań jest uprawniona do przetwarzania informacji, w tym danych osobowych, oraz ich wymiany z właściwymi organami i instytucjami krajowymi Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi.
2. Żandarmeria Wojskowa w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), przetwarza dane oso-

bowe w zakresie niezbędnym do realizacji zadań ustawowych związanych z zapobieganiem i zwalczaniem przestępstw oraz przestępstw skarbowych, a także wykroczeń oraz wykroczeń skarbowych, w tym dane osobowe, o których mowa w art. 14 ust. 1 tej ustawy. Dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA.

3. Żandarmeria Wojskowa w celu realizacji zadań, o których mowa w art. 4 ust. 1 pkt 3a i ust. 4, może przetwarzać dane biometryczne lub dane genetyczne, o których mowa w art. 4 pkt 2 i 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości:

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

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

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

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

2) posiadają zabezpieczenie techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania;
3) jest to uzasadnione specyfiką lub zakresem wykonywania zadań albo prowadzonej działalności.

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

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

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

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

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

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

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

13. Żandarmeria Wojskowa udostępnia właściwym podmiotom informacje, o których mowa w art. 4 ust. 2 pkt 19, w tym dane

osobowe, na pisemny wniosek, który powinien zawierać podstawę prawną, przeznaczenie, wskazanie okresu oraz zakresu danych podlegających sprawdzeniu, a także podpis upoważnionej osoby.

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

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

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

17. Minister Obrony Narodowej określi, w drodze rozporządzenia:

1) zasady przetwarzania danych biometrycznych oraz danych genetycznych, w tym w szczególności wymazów ze śluzówki policzków, odcisków linii papilarnych oraz zdjęć sygnalitycznych osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, osób o nieustalonej tożsamości lub osób usiłujących ukryć swoją tożsamość, i sposób ich przekazywania innym organom uprawnionym na podstawie przepisów odrębnych, a także wzory wykorzystywanych dokumentów, uwzględniając

przypadki i sposoby pobierania odcisków linii papilarnych, przeprowadzania wywiadu daktyloskopijnego oraz wykonywania zdjęć sygnalitycznych, kierując się potrzebą ochrony tych danych przed nieuprawnionym dostępem;

2) tryb pobierania odcisków linii papilarnych lub wymazów ze śluzówki policzków od żołnierzy i pracowników Żandarmerii Wojskowej oraz sposób przeprowadzania i dokumentowania czynności związanych z ich przetwarzaniem, uwzględniając konieczność wyeliminowania pozostawionych przez nich śladów;
3) zbiory danych, w których Żandarmeria Wojskowa przetwarza dane osobowe, uwzględniając ich przeznaczenie i zakres;
4) kryteria oceny danych pod kątem przesłanek dalszego przetwarzania, kierując się ich przydatnością do realizacji zadań związanych z zapobieganiem i zwalczaniem przestępczości.

Artykuł 73. Zmiany w ustawie o transporcie drogowym.

W ustawie z dnia 6 września 2001 r. o transporcie drogowym (Dz.U. z 2019 r. poz. 58 i 60) wprowadza się następujące zmiany:

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

1a. Inspekcja w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), jest uprawniona do przetwarzania informacji, w tym danych osobowych, oraz ich wymiany z właściwymi organami i instytucjami krajowymi, Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi.

1b. Inspekcja może przekazać dane osobowe państwu trzeciemu lub organizacjom międzynarodowym, na ich wniosek, w przypadku gdy są spełnione warunki przekazywania informacji określone w art. 18a–18d ustawy z dnia 16 września 2011 r. o wymia-

nie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2018 r. poz. 484 oraz z 2019 r. poz. 125).

2) po art. 56 dodaje się art. 56a w brzmieniu:
„Art. 56a. Administratorem danych osobowych przetwarzanych w związku z realizacją czynności określonych w art. 56 ust. 1, w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jest Główny Inspektor Transportu Drogowego lub wojewódzki inspektor transportu drogowego.”.

Artykuł 74. Zmiany w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2018 r. poz. 2387, 2245 i 2399 oraz z 2019 r. poz. 53) w art. 34 ust. 1 otrzymuje brzmienie:

„1. W zakresie swojej właściwości Agencje mogą zbierać, także niejawnie, wszelkie dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), a także korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je bez wiedzy i zgody osoby, której te dane dotyczą.”

Artykuł 75. Zmiany w ustawie Prawo o ustroju sądów administracyjnych.

W ustawie z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych (Dz.U. z 2018 r. poz. 2107) po art. 12 dodaje się art. 12a i art. 12b w brzmieniu:

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

§ 2. Do przetwarzania danych osobowych w postępowaniach sądowych przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej "rozporządzeniem 2016/679", nie stosuje się.

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

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

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

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

Artykuł 76. Zmiany w ustawie o transporcie kolejowym.

W ustawie z dnia 28 marca 2003 r. o transporcie kolejowym (Dz.U. z 2017 r. poz. 2117, z późn. zm.[17)]) po art. 60 dodaje się art. 60a w brzmieniu:

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

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

2. Administratorem danych osobowych przetwarzanych przez straż ochrony kolei jest komendant straży ochrony kolei."

Artykuł 77. Zmiany w ustawie o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych.

W ustawie z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz.U. z 2018 r. poz. 473 i 2448) w art. 104 w ust. 1 pkt 10 otrzymuje brzmienie:

„10) Policji, o ile są niezbędne w toczącym się postępowaniu lub na potrzeby wykonywania czynności operacyjno-rozpoznawczych na zasadach i w trybie określonym w art. 20 ust. 1d i 1e ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2017 r. poz. 2067, z późn. zm.[18)]);".

Artykuł 78. Zmiany w ustawie o Centralnym Biurze Antykorupcyjnym.

W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2018 r. poz. 2104 i 2399 oraz z 2019 r. poz. 53) w art. 22a ust. 1 otrzymuje brzmienie:

„1. W granicach zadań, o których mowa w art. 2 ust. 1, CBA może przetwarzać dane osobowe, w tym dane wskazane w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), bez wiedzy i zgody osoby, której te dane dotyczą."

Artykuł 79. Zmiany w ustawie o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

W ustawie z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2017 r. poz. 1978, z późn. zm.[19)]) w art. 38 ust. 1 otrzymuje brzmienie:

„1. W zakresie swojej właściwości SKW i SWW mogą zbierać, także niejawnie, wszelkie dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), a także korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je bez wiedzy i zgody osoby, której te dane dotyczą."

Artykuł 80. Zmiany w ustawie o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym.

W ustawie z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz.U. z 2018 r. poz. 2162 i 2354) wprowadza się następujące zmiany:

1) w art. 2:
   a) pkt 1 otrzymuje brzmienie:
      „1) bezpośrednim dostępie – rozumie się przez to dokonywanie wpisów oraz wgląd do danych przetwarzanych poprzez Krajowy System Informatyczny (KSI), realizowany w sposób bezpośredni przez organ wskazany w ustawie;”,
   b) pkt 7 otrzymuje brzmienie:
      „7) informacjach uzupełniających – rozumie się przez to wszelkie informacje, wymieniane za pośrednictwem biur SIRENE między krajowymi a zagranicznymi organami uprawnionymi do przetwarzania danych SIS, niezbędne przy dokonywaniu wpisów do Systemu Informacyjnego Schengen lub w celu umożliwienia podjęcia odpowiednich działań, w przypadkach gdy w wyniku przeglądania danych SIS odnaleziono osoby lub przedmioty, których dotyczą wpisy;”,
   c) pkt 11 otrzymuje brzmienie:
      „11) Krajowym Systemie Informatycznym (KSI) – rozumie się przez to zespół współpracujących ze sobą urządzeń, procedur przetwarzania informacji i narzędzi programowych (oprogramowania) zastosowanych w celu przetwarzania danych oraz infrastrukturę telekomunikacyjną, umożliwiające organom administracji publicznej i organom wymiaru sprawiedliwości przetwarza-

nie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym;",

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

e) pkt 18 otrzymuje brzmienie:
„18) przetwarzaniu danych – rozumie się przez to przetwarzanie danych będących danymi osobowymi, jak również jakiekolwiek operacje wykonywane na danych niebędących danymi osobowymi, takie jak: zbieranie, wpisywanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie; w odniesieniu do danych osobowych przetwarzanych w celach, o których mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), stosuje się przepisy tej ustawy, a w przypadku danych osobowych przetwarzanych w innych celach przepisy rozporządzenia 2016/679;",

f) dodaje się pkt 19 w brzmieniu:
„19) rozporządzeniu 2016/679 – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).";

2) tytuł rozdziału 2 otrzymuje brzmienie:
„Organy i służby uprawnione do przetwarzania danych”
3) w art. 6 pkt 4 otrzymuje brzmienie:
„4) sprawdzenia na przejściach granicznych tożsamości posiadacza wizy, autentyczności wizy lub spełnienia warunków wjazdu na terytorium Państw Członkowskich zgodnie z art. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.Urz. UE L 77/1 z 23.03.2016) przysługuje Straży Granicznej i Służbie Celno-Skarbowej;”;
4) użyty w tytule rozdziału 3, w art. 11 w ust. 1, w art. 22 w ust. 3, w art. 23 w ust. 4, w art. 24, w art. 25 w ust. 1–4, w art. 27 w ust. 1 w pkt 4 i 5, w ust. 2 w pkt 1, 5 i 9 oraz w art. 28 w różnej liczbie i w różnym przypadku wyraz ”wykorzystywania” zastępuje się użytym w odpowiedniej liczbie i przypadku wyrazem ”przetwarzania”;
5) art. 8–10 otrzymują brzmienie:

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

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

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

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

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

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

8) art. 30–32 otrzymują brzmienie:

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

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

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

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

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

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

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

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

1) uznać zgłoszone zastrzeżenia za niezasadne i podtrzymać zalecenia pokontrolne;

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

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

8) w art. 34:
   a) ust. 1 otrzymuje brzmienie:
      „1. W przypadku dokonywania jakichkolwiek zmian w Krajowym Systemie Informatycznym (KSI) po jego uruchomieniu centralny organ techniczny KSI jest obowiązany przed wdrożeniem tych zmian do uzyskania pisemnej opinii ministra właściwego do spraw wewnętrznych w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 4 i art. 9 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz w art. 4 i art. 9 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), oraz opinii Prezesa Urzędu Ochrony Danych Osobowych."
   b) ust. 5 otrzymuje brzmienie:
      „5. Uzyskanie opinii Prezesa Urzędu Ochrony Danych Osobowych, o której mowa w ust. 1, następuje w zakresie i w trybie określonych w art. 30–32."

Artykuł 81. Zmiany w ustawie o bezpieczeństwie imprez masowych.

W ustawie z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz.U. z 2018 r. poz. 1870 oraz z 2019 r. poz. 61) wprowadza się następujące zmiany:

1) w art. 1 pkt 4 otrzymuje brzmienie:
   „4) zasady przetwarzania informacji dotyczących bezpieczeństwa imprez masowych, w tym danych osobowych;";
2) art. 10 otrzymuje brzmienie:
   „Art. 10. Organizator masowej imprezy sportowej, innej niż wymieniona w rozdziale 3, może odmówić na nią wstępu i przebywania osobie, której dane znajdują się w zbiorze danych, o którym mowa w art. 37 pkt 2, lub objętej zakazem klubowym lub zakazem zagranicznym.";
3) w art. 11 w ust. 3 po wyrazach "co najmniej 30 dni," dodaje się wyrazy "nie dłużej jednak niż 90 dni,";
4) w art. 13:
   a) ust. 2b i 2c otrzymują brzmienie:
      2b. Administratorami danych osobowych przetwarzanych w systemach, o których mowa w ust. 2a, są właściwe podmioty zarządzające tymi rozgrywkami.
      2c. Kompatybilność oznacza, iż elektroniczne systemy, o których mowa w ust. 2, muszą być podłączone do systemów, o których mowa w ust. 2a, oraz działać na podstawie numeru PESEL, a w razie gdy nie został on nadany – rodzaju, serii i numeru dokumentu potwierdzającego tożsamość, po przekazaniu danych osobowych, o których mowa w ust. 4.
   b) w ust. 4 wprowadzenie do wyliczenia otrzymuje brzmienie:
      „Zakres przetwarzanych danych osobowych osób uczestniczących w meczu piłki nożnej obejmuje:"
   c) ust. 7–14 otrzymują brzmienie:

7. Przetwarzanie informacji, w tym danych osobowych, w systemach, o których mowa w ust. 2 i 2a, ma na celu zapewnienie bezpieczeństwa osób uczestniczących w meczu piłki nożnej.
8. Zakres informacji, w tym danych osobowych, przetwarzanych w systemie, o którym mowa w ust. 2a pkt 1, obejmuje:
1) dane osobowe określone w ust. 4,
2) dane osobowe, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c,
3) informacje o zastosowanych zakazach, w tym przekazane przez organizatorów imprez masowych

– w zakresie, w jakim te informacje, w tym dane osobowe, dotyczą uczestników meczów piłki nożnej rozgrywanych w ramach najwyższej ligowej klasy rozgrywkowej rywalizacji mężczyzn.
9. Zakres informacji, w tym danych osobowych, przetwarzanych w systemie, o którym mowa w ust. 2a pkt 2, obejmuje:
1) dane osobowe określone w ust. 4,
2) dane osobowe, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c,
3) informacje o zastosowanych zakazach, w tym przekazane przez organizatorów imprez masowych

– w zakresie, w jakim te informacje, w tym dane osobowe, dotyczą uczestników meczów piłki nożnej rozgrywanych w drugiej i trzeciej najwyższej ligowej klasie rozgrywkowej rywalizacji mężczyzn.
10. Informacje, w tym dane osobowe, do systemów, o których mowa w ust. 2 i 2a, przekazują w zakresie swojej właściwości:
1) właściwy polski związek sportowy;
2) właściwy podmiot zarządzający rozgrywkami;
3) organizator meczu piłki nożnej;
4) Komendant Główny Policji;
5) podmiot uprawniony do dystrybucji biletów.

11. Podmioty przekazujące informacje, w tym dane osobowe, do systemów, o których mowa w ust. 2 i 2a, są odpowiedzialne za kompletność, aktualność oraz prawdziwość przekazywanych informacji.
12. Dostęp do informacji, w tym danych osobowych, przetwarzanych w systemach, o których mowa w ust. 2 i 2a, w zakresie swoich kompetencji, posiadają:
1) właściwy polski związek sportowy;
2) właściwy podmiot zarządzający rozgrywkami;
3) organizator meczu piłki nożnej;
4) podmiot uprawniony do dystrybucji biletów;
5) Policja, w zakresie weryfikacji poprawności informacji o osobach, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c, oraz w związku z prowadzonym postępowaniem przygotowawczym lub czynnościami operacyjno-rozpoznawczymi.

13. Informacje, w tym dane osobowe, przetwarzane w systemach, o których mowa w ust. 2 i 2a, są przechowywane nie dłużej niż przez okres 2 lat od dnia ostatniego zakupu biletu wstępu przez uczestnika meczu piłki nożnej lub przekazania mu innego dokumentu uprawniającego do przebywania na meczu piłki nożnej.
13a. Jeżeli informacje, w tym dane osobowe, przetwarzane w systemach, o których mowa w ust. 2 i 2a, dotyczą osoby, wobec której zostało wydane orzeczenie lub zakaz, o których mowa w art. 22 ust. 1 pkt 1 lit. a–c, wówczas okres, o którym mowa w ust. 13, liczy się od dnia upływu okresu obowiązywania zakazu lub okresu, na który orzeczono dany środek.
14. Informacje, w tym dane osobowe, przetwarzane w systemach, o których mowa w ust. 2 i 2a, podlegają usunięciu, jeżeli:
1) zostały zgromadzone z naruszeniem ustawy;

2) okazały się niekompletne, nieaktualne lub nieprawdziwe;
3) upłynął okres, o którym mowa w ust. 13."

5) w art. 15:
   a) w ust. 1 po wyrazie "danych" dodaje się wyraz "osobowych",
   b) w ust. 2 po wyrazie "dane" dodaje się wyraz "osobowe";
6) tytuł rozdziału 7 otrzymuje brzmienie: „Zasady przetwarzania informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprezy masowej"
7) art. 35 otrzymuje brzmienie:
   „Art. 35. 1. Przetwarzanie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych odbywa się w celu zapobiegania przestępstwom i wykroczeniom związanym z tymi imprezami oraz ich zwalczania.
   2. Przetwarzanie danych osobowych może odbywać się bez obowiązku informowania osób, których one dotyczą.
8) w art. 36 ust. 1 i 2 otrzymują brzmienie:
   1. Organem administracji rządowej właściwym w sprawach przetwarzania informacji, w tym danych osobowych, dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, jest Komendant Główny Policji, zwany dalej "Komendantem".
   2. Komendant przetwarza informacje, w tym dane osobowe, dotyczące imprez masowych innych niż masowe imprezy sportowe, w tym mecze piłki nożnej, w zakresie obejmującym dane osobowe o osobach, o których mowa w art. 22 ust. 1 pkt 1 lit. a i b, oraz o terminach i miejscach przeprowadzania tych imprez.
9) art. 37 otrzymuje brzmienie:
   „Art. 37. Do zadań Komendanta należy w szczególności:
   1) przetwarzanie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych;
   2) prowadzenie zbioru danych dotyczących bezpieczeństwa imprez masowych;

3) opracowywanie analiz informacji dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej;
4) zapewnienie bezpieczeństwa przetwarzanych informacji dotyczących bezpieczeństwa imprez masowych, w tym, zgodnie z przepisami ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), bezpieczeństwa danych osobowych;
5) współpraca z podmiotami zagranicznymi w zakresie, o którym mowa w pkt 1–3.";

9) w art. 38:
a) w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:
„Podmiotami uprawnionymi w zakresie swoich kompetencji do otrzymywania od Komendanta informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych, zwanymi dalej "podmiotami uprawnionymi", są:"
b) ust. 2 i 3 otrzymują brzmienie:
2. Organizatorzy imprez masowych innych niż masowe imprezy sportowe, w tym mecze piłki nożnej, są uprawnieni w zakresie swoich zadań ustawowych do otrzymywania od Komendanta informacji, w tym danych osobowych, dotyczących osób, o których mowa w art. 22 ust. 1 pkt 1 lit. a i b.
3. Komendanci wojewódzcy (Komendant Stołeczny) Policji i komendanci powiatowi (rejonowi, miejscy) Policji przekazują podmiotom, o których mowa w ust. 1 pkt 1–15, na wniosek tych podmiotów, informacje, w tym dane osobowe, o których mowa w art. 22 ust. 1 pkt 1 lit. a i b i art. 40, dotyczące imprez masowych organizowanych na obszarze działania tych komendantów. Przepisy art. 42 ust. 1, 4 i 5, art. 43, art. 44 ust. 1, 2 i 4, art. 45, art. 46 oraz art. 47 stosuje się odpowiednio.

11) art. 39 otrzymuje brzmienie:
„Art. 39. 1. Podmiotami zobowiązanymi do przekazywania Komendantowi informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych, zwanymi dalej ”podmiotami zobowiązanymi”, są podmioty, o których mowa w art. 38 ust. 1 pkt 1–15, oraz:
1) Biuro Informacyjne Krajowego Rejestru Karnego oraz sądy, w których zapadło prawomocne orzeczenie o ukaraniu za wykroczenie karą inną niż kara aresztu;
2) związki sportowe;
3) organizatorzy;
4) właściciele obiektów, na terenie których organizowane są masowe imprezy sportowe, w tym mecze piłki nożnej;
5) organizatorzy turystyki;
6) krajowi przewoźnicy realizujący publiczny transport zbiorowy.

2. Podmioty zobowiązane przekazują komendantom wojewódzkim (Komendantowi Stołecznemu) Policji i komendantom powiatowym (rejonowym, miejskim) Policji, na wniosek komendantów, informacje, w tym dane osobowe, o których mowa w art. 22 ust. 1 pkt 1 lit. a i b i art. 40, dotyczące imprez masowych organizowanych na obszarze działania tych komendantów. Przepisy art. 41, art. 42 ust. 1–3 oraz art. 45 stosuje się odpowiednio.

12) w art. 40 wprowadzenie do wyliczenia otrzymuje brzmienie:
„Zakres przetwarzanych informacji, w tym danych osobowych, dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, zawiera dane:”

12) art. 41–43 otrzymują brzmienie:
„Art. 41. 1. Podmioty zobowiązane, z zastrzeżeniem ust. 2, przekazują Komendantowi informacje, w tym dane osobowe, dotyczące bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, niezwłocznie po ich otrzymaniu, nie później jednak niż w ciągu 24 godzin od chwili ich otrzymania.

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

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

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

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

4. Komendant udziela informacji na kartach odpowiedzi.

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

6. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób przekazywania informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez maso-

wych przez podmioty zobowiązane, wzory kart rejestracyjnych, karty zapytania oraz karty odpowiedzi, biorąc pod uwagę dane, jakie muszą znaleźć się na kartach, oznaczenia podmiotu uprawnionego oraz podmiotu zobowiązanego, treść informacji, o której mowa w ust. 2, oraz zapytania, o którym mowa w ust. 3, jak również uzasadnienia, o którym mowa w art. 43, a także konieczność zapewnienia bezpieczeństwa przekazywanych informacji, w tym dane osobowe, w szczególności przed dostępem osób nieuprawnionych.

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

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

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

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

15) art. 46–49 otrzymują brzmienie:
„Art. 46. Przetwarzanie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych może być doko-

nywane przy wykorzystaniu urządzeń i systemów teleinformatycznych, kartotek, wykazów i zbiorów ewidencyjnych.

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

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

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

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

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

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

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

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

Artykuł 82. Zmiany w ustawie o Służbie Więziennej.

W ustawie z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz.U. z 2018 r. poz. 1542, 1669, 2245 i 2399) wprowadza się następujące zmiany:

1) w art. 2 w ust. 2 po pkt 7 dodaje się pkt 7a w brzmieniu:
   „7a) prowadzenie Centralnej Bazy Danych Osób Pozbawionych Wolności, zwanej dalej ”Centralną Bazą”;”;
2) art. 24 otrzymuje brzmienie:
   „Art. 24. 1. Służba Więzienna, w celu realizacji zadań, o których mowa w art. 2 ust. 1, 2 i 2b, oraz zadań wynikających z odrębnych ustaw, jest uprawniona do przetwarzania:
   1) informacji innych niż dane osobowe,
   2) danych osobowych, a w celu realizacji zadań, o których mowa w art. 2 ust. 1 i 2, także danych, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125)

   – niezbędnych do realizacji tych zadań.

   2. Zasady i warunki przetwarzania danych osobowych na podstawie niniejszej ustawy przez Służbę Więzienną w celu wykonywania orzeczeń wydanych w postępowaniu karnym, postępowaniu w sprawach o przestępstwa skarbowe, w sprawach o wykroczenia lub wykroczenia skarbowe oraz wykonywania kar porządkowych i środków przymusu skutkujących pozbawieniem wolności, a także ochrony przed zagrożeniami dla bezpieczeństwa publicznego i porządku publicznego i zapobiegania takim zagrożeniom reguluje ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z wyjątkami określonymi w niniejszej ustawie.

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

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

1) obecnie lub uprzednio pozbawionych wolności w zakładach karnych i aresztach śledczych – w zakresie związanym z pozbawieniem wolności w tych zakładach i aresztach, w tym w zakresie niezbędnym do:
   a) wykonania orzeczenia, zgodnie z zasadami określonymi w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
   b) zapewnienia porządku i bezpieczeństwa w zakładach karnych i aresztach śledczych,
   c) ochrony społeczeństwa przed przestępczością,
   d) wykonania zadań wynikających z odrębnych ustaw;
2) które mają być pozbawione wolności w zakładach karnych i aresztach śledczych, w wykonaniu orzeczenia wydanego przez właściwy organ i przesłanego przez sąd do zakładu karnego lub aresztu śledczego, w celu realizacji czynności, o których mowa w art. 79 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy – w zakresie niezbędnym do wykonania orzeczenia zgodnie z zasadami określonymi w tym kodeksie;
3) wobec których kary, środki karne i środki zabezpieczające są wykonywane w systemie dozoru elektronicznego – w zakresie niezbędnym do wykonania zadania, o którym mowa w art. 2 ust. 2 pkt 9;
4) innych niż wymienione w pkt 1–3, związane z realizacją wobec tych osób czynności przewidzianych w przepisach odrębnych oraz wykonywaniem praw lub obowiązków osób pozbawionych wolności, w tym dane osobowe:
   a) pokrzywdzonych i świadków – w zakresie niezbędnym do realizacji zadań, o których mowa w art. 168a § 1 i 6 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,

b) osób ubiegających się o wstęp oraz opuszczających teren jednostek organizacyjnych – w zakresie niezbędnym do zapewnienia realizacji czynności wykonywanych przez te osoby na terenie jednostek organizacyjnych,
c) osób zakłócających spokój lub naruszających porządek i bezpieczeństwo jednostek organizacyjnych – w zakresie niezbędnym dla realizacji czynności przewidzianych w przepisach odrębnych,
d) rodziny oraz innych osób bliskich – w zakresie realizacji praw przewidzianych w przepisach odrębnych;

5) funkcjonariuszach i pracownikach oraz innych osobach pełniących służbę lub zatrudnionych w organach władzy publicznej, dokonujących czynności z udziałem lub wobec osób, o których mowa w pkt 1–3 lub których dane osobowe zawarto w dokumentach przekazanych Służbie Więziennej – w zakresie niezbędnym do wykonania obowiązków i zadań wymienionych w pkt 1–3.

5. Osobie pozbawionej wolności nie udostępnia się:

1) jej akt osobowych, prowadzonych przez administrację zakładu karnego lub aresztu śledczego, z zastrzeżeniem art. 102 pkt 9 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy;
2) informacji przetwarzanych w Centralnej Bazie lub innym zbiorze danych prowadzonym w systemie teleinformatycznym, w zakresie odpowiadającym informacjom zawartym w aktach, o których mowa w pkt 1, uzasadniającym ograniczenie dostępu do tych akt.
3) po art. 24 dodaje się art. 24a i art. 24b w brzmieniu:

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

2. Służba Więzienna, na pisemny i uzasadniony wniosek osoby najbliższej w postaci papierowej lub elektronicznej, udostępnia dane osobowe osoby obecnie pozbawionej wolności, za pisemną zgodą tej osoby.
3. Służba Więzienna udziela informacji o osobie pozbawionej wolności, która zmarła:
1) podmiotom ustawowo uprawnionym, na zasadach określonych w ust. 1;
2) osobie najbliższej, na pisemny i uzasadniony wniosek tej osoby;
3) osobie innej niż najbliższa, tylko jeżeli zgon nastąpił w zakładzie karnym lub areszcie śledczym, w zakresie informacji o zgonie, jego miejscu i dacie, po wykazaniu w pisemnym wniosku interesu prawnego w potwierdzeniu tych faktów.
4. Przepisy ust. 3 pkt 2 i 3 nie naruszają zasady udostępniania dokumentacji medycznej zmarłego, o której mowa w art. 26 ust. 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2017 r. poz. 1318 i 1524 oraz z 2018 r. poz. 1115, 1515, 2219 i 2429).
5. Minister Sprawiedliwości określi, w drodze rozporządzenia, tryb i sposób składania oraz wzór wniosku o udzielenie informacji lub udostępnienie danych osobowych o osobie obecnie lub uprzednio pozbawionej wolności w zakładzie karnym lub areszcie śledczym, zawierającego oznaczenie podmiotu ubiegającego się o udzielenie informacji lub udostępnienie danych osobowych, podstawę prawną, zakres udostępnianych danych i udzielanych informacji oraz danych identyfikujących osobę pozbawioną wolności, a w przypadku osoby najbliższej albo osoby innej niż najbliższa – uzasadnienie wniosku, mając na względzie w szczególności zakres uprawnień ustawowych ubiegających się podmiotów.
Art. 24b. 1. Służba Więzienna w związku z realizacją zadań, o których mowa w art. 2 ust. 1, 2 i 2b, oraz zadań wynikających z odrębnych ustaw jest uprawniona do przetwarzania danych

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

2. Przetwarzanie danych osobowych, o których mowa w ust. 1, następuje z wyłączeniem stosowania art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[21)]), zwanego dalej"rozporządzeniem 2016/679", w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowiązaniu funkcjonariuszy lub pracowników do zachowania przetwarzanych danych w poufności.

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

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

4) uchyla się art. 25;

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

„Rozdział 4a Centralna Baza

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

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

1) osób, o których mowa w art. 24 ust. 4 pkt 1, obejmujące:
   a) dane osobowe, takie jak: imiona, nazwisko, poprzednio używane imiona i nazwiska, pseudonimy, imiona i nazwiska rodziców, nazwisko rodowe matki, datę i miejsce urodzenia, numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), aktualne i poprzednie adresy zameldowania, zamieszkania lub pobytu, także czasowego, obywatelstwo,
   b) informacje pozwalające na identyfikację osoby pozbawionej wolności, w tym dane biometryczne,
   c) informacje wynikające z orzeczeń i innych dokumentów przesłanych przez sąd do zakładu karnego lub aresztu śledczego, w tym informacje, o których mowa w art. 11 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
   d) informacje dotyczące stawienia się skazanego lub ukaranego do odbycia kary we właściwym zakładzie karnym lub areszcie śledczym,
   e) informacje dotyczące osoby pozbawionej wolności zebrane w trybie art. 14 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
   f) informacje związane z pobytem osoby pozbawionej wolności w zakładzie karnym lub areszcie śledczym, w szczególności:
      – informacje o wprowadzonych do wykonania orzeczeniach oraz okresach wykonywania pozbawienia wolności, w tym także poza zakładem karnym lub aresztem śledczym, oraz inne informacje mające wpływ na ustalenie terminu końca kary lub środka przymusu,

- informacje niezbędne do dokonania prawidłowej klasyfikacji, rozmieszczenia wewnątrz zakładu karnego lub aresztu śledczego oraz indywidualnego postępowania zmierzającego do realizacji celów, jakim ma służyć wykonanie kar pozbawienia wolności, środków przymusu skutkujących pozbawieniem wolności oraz tymczasowego aresztowania, w tym w szczególności informacje:
- o których mowa w art. 82 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
- wynikające z badań osobopoznawczych, o których mowa w art. 82 § 3 i art. 212c § 1 zdanie pierwsze ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy,
- dotyczące diagnoz psychologicznych oraz udzielonej pomocy psychologicznej i terapeutycznej,
- informacje o zakwalifikowaniu osoby pozbawionej wolności jako osoby stwarzającej poważne zagrożenie społeczne albo poważne zagrożenie dla bezpieczeństwa zakładu karnego lub aresztu śledczego,
- informacje o objęciu osoby pozbawionej wolności szczególną ochroną w warunkach zwiększonej izolacji i zabezpieczenia,
- dane dotyczące zdrowia, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie zdrowia,
- informacje dotyczące wykształcenia, zawodu, innych kwalifikacji zawodowych oraz nauki, w tym miejsca jej pobierania,
- informacje dotyczące wniosków, skarg i próśb złożonych przez osobę pozbawioną wolności,
- oznaczenia i cechy identyfikacyjne dokumentów, w tym dokumentów stwierdzających tożsamość,

przekazanych do depozytu zakładu karnego lub aresztu śledczego,
- informacje o rozmieszczeniu wewnątrz zakładu karnego lub aresztu śledczego, przenoszeniu między zakładami karnymi i aresztami śledczymi, o przebywaniu poza terenem tych zakładów lub aresztów pod konwojem, o przepustce lub innym czasowym zezwoleniu na opuszczenie terenu zakładu karnego lub aresztu śledczego, wydaniu poza teren tego zakładu lub aresztu, w tym do udziału w czynnościach procesowych, o ucieczce z zakładu karnego lub aresztu śledczego, a także o tym, że w wyznaczonym terminie osoba pozbawiona wolności nie powróciła z przepustki lub innego czasowego zezwolenia na opuszczenie terenu zakładu karnego lub aresztu śledczego,
- informacje dotyczące zgonu osoby pozbawionej wolności w zakładzie karnym lub areszcie śledczym,
- informacje dotyczące zatrudnienia osoby pozbawionej wolności,
- informacje w zakresie spraw prowadzonych w szczególności w związku z postępowaniem o zezwolenie na odbywanie kary w systemie dozoru elektronicznego, warunkowe przedterminowe zwolnienie oraz przerwę w wykonaniu kary,

g) informacje związane ze zwolnieniem osoby pozbawionej wolności z zakładu karnego lub aresztu śledczego, w tym dotyczące zwolnienia skazanego lub ukaranego na przerwę w wykonaniu kary,
h) inne informacje, jeżeli wynika to z przepisów szczególnych;

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

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

Art. 25b. 1. Dyrektor Generalny:
1) prowadzi w systemie teleinformatycznym Centralną Bazę;
2) jest administratorem informacji, w tym danych osobowych, przetwarzanych w Centralnej Bazie;
3) dokonuje weryfikacji przydatności informacji w Centralnej Bazie, mając na względzie ich niezbędność do realizacji ustawowych zadań wynikającą z rodzaju informacji oraz upływu czasu;
4) zapewnia:
   a) bezpieczeństwo Centralnej Bazy, w szczególności zabezpiecza przetwarzane w niej informacje przed nieuprawnionym dostępem, zniszczeniem oraz utratą,
   b) utrzymanie i niezbędne modyfikacje Centralnej Bazy.

2. Informacje w Centralnej Bazie:
1) przetwarza się przez okres, w którym są niezbędne do realizacji ustawowych zadań wykonywanych przez Służbę Więzienną. Dyrektor Generalny dokonuje, nie rzadziej niż co

5 lat, weryfikacji potrzeby dalszego przetwarzania tych informacji, ustalając informacje zbędne;

2) uznane za zbędne, mogą być przetwarzane tylko w celu realizacji obowiązku, o którym mowa w pkt 3. Jeżeli przemawia za tym prawidłowość informacji przetwarzanych w Centralnej Bazie, informacje uznane za zbędne mogą być przekształcone w sposób uniemożliwiający przyporządkowanie poszczególnych danych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań;
3) stanowią materiały archiwalne w rozumieniu art. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2018 r. poz. 217, 357, 398 i 650 oraz z 2019 r. poz. 55).

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

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

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

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

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

2. O zgodę, o której mowa w ust. 1, występuje:
1) Minister Sprawiedliwości – w imieniu podmiotów, o których mowa w ust. 1 pkt 1;
2) Prokurator Generalny – w imieniu podmiotów, o których mowa w ust. 1 pkt 2.

Art. 25d. 1. Dyrektor Generalny wyraża zgodę, w drodze decyzji, na wielokrotne, nieograniczone w czasie udostępnianie informacji z Centralnej Bazy, z wyjątkiem danych dotyczących zdrowia osób obecnie lub uprzednio pozbawionych wolności oraz informacji dotyczących diagnoz psychologicznych oraz udzielonej im pomocy psychologicznej i terapeutycznej, za pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku, podmiotom wymienionym w art. 25c ust. 1, jeżeli podmioty te spełniają łącznie następujące warunki:
1) posiadają urządzenia umożliwiające odnotowanie w systemie kto, kiedy, w jakim celu oraz jakie informacje uzyskał;

2) posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie informacji niezgodnie z celem ich uzyskania;
3) jest to uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności;
4) po stronie tych podmiotów oraz Służby Więziennej istnieją warunki techniczne.

2. Warunki udostępniania informacji podmiotowi wymienionemu w art. 25c ust. 1 pkt 16 określa Dyrektor Generalny, w decyzji, o której mowa w ust. 1, mając na względzie:
1) że informacje z Centralnej Bazy udostępniane są Rzecznikowi Praw Obywatelskich lub osobie przez niego upoważnionej na terenie zakładu karnego lub aresztu śledczego;
2) konieczność wprowadzenia zabezpieczeń technicznych i organizacyjnych uniemożliwiających wykorzystanie informacji niezgodnie z celem ich uzyskania;
3) zasady przetwarzania informacji w Centralnej Bazie przez Służbę Więzienną.

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

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

Art. 25f. 1. Dyrektor Generalny, w drodze decyzji, odmawia wyrażenia zgody na wielokrotne, nieograniczone w czasie, udostępnianie informacji z Centralnej Bazy, za pośrednictwem systemu teleinformatycznego, bez konieczności każdorazowego składania wniosku, jeżeli:
1) podmiot występujący z wnioskiem nie jest podmiotem wymienionym w art. 25c ust. 1 pkt 3–15 lub ust. 2;

2) podmiot wymieniony w art. 25c ust. 1 pkt 3–14 lub ust. 2 nie wykazał, że spełnione są warunki określone w art. 25d ust. 1 pkt 1–3;
3) nie istnieją warunki techniczne po stronie podmiotów wymienionych w art. 25c ust. 1 pkt 1–14 lub Służby Więziennej;
4) podmiot wymieniony w art. 25c ust. 1 pkt 16 nie spełnił warunków określonych przez Dyrektora Generalnego, o których mowa w art. 25d ust. 2.

2. Dyrektor Generalny cofa w drodze decyzji zgodę, o której mowa w art. 25d ust. 1, jeżeli zadania podmiotu, który uzyskał zgodę, nie czynią niezbędnym takiego dostępu lub ustalono, że podmiot taki nie spełnia warunków, o których mowa w art. 25d ust. 1–4, albo podmiot wymieniony w art. 25c ust. 1 pkt 16 nie spełnia warunków określonych przez Dyrektora Generalnego, o których mowa w art. 25d ust. 2.

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

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

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

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

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

1) warunki, o których mowa w art. 25d ust. 1, w tym zwłaszcza konieczność wykazania przez podmioty, o których mowa

w art. 25c ust. 1 pkt 3–14 i ust. 2, informacji, których udostępnianie jest niezbędne dla wykonywania zadań określonych w odrębnych ustawach, oraz konieczność wykazania przez te podmioty odpowiedniego poziomu zabezpieczeń technicznych i organizacyjnych;

2) warunki, o których mowa w art. 25d ust. 2, w przypadku podmiotu wymienionego w art. 25c ust. 1 pkt 16;
3) potrzebę zapewnienia sprawności i bezpieczeństwa udostępniania informacji z Centralnej Bazy, za pośrednictwem systemu teleinformatycznego, oraz ochrony tych informacji przed nieuprawnionym dostępem.

Art. 25h. Minister Sprawiedliwości i minister właściwy do spraw wewnętrznych określą, w drodze rozporządzenia, zakres informacji w Centralnej Bazie, do których bezpośredni dostęp posiada punkt kontaktowy, o którym mowa w art. 4 ust. 1 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2018 r. poz. 484 oraz z 2019 r. poz. 125), w celu ich wymiany z organami ścigania innych państw na zasadach i w trybie określonych w przepisach tej ustawy, mając na względzie konieczność zapewnienia dostępu do informacji niezbędnych do wykonywania zadań przez ten punkt kontaktowy oraz potrzebę zapewnienia bezpieczeństwa i ochrony danych osobowych przetwarzanych w Centralnej Bazie.

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

1) przekazuje, za pośrednictwem systemu teleinformatycznego, informacje o osobach pozbawionych wolności do Krajowego Rejestru Karnego, w zakresie określonym w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz.U. z 2018 r. poz. 1218 i 1544 oraz z 2019 r. poz. 60) oraz w przepisach wydanych na podstawie art. 12 ust. 3 tej ustawy;

2) może przekazywać, za pośrednictwem systemu teleinformatycznego, informacje określone w odrębnych przepisach, do uprawnionych podmiotów, realizując ustawowe zadania Służby Więziennej wynikające z tych przepisów.

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

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

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

Artykuł 83. Zmiany w ustawie o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych.

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

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

Artykuł 84. Zmiany w ustawie o ochronie informacji niejawnych.

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

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

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

Artykuł 85. Zmiany w ustawie o wymianie informacji z organami ścigania państw członkowskich UE.

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

1) tytuł ustawy otrzymuje brzmienie:
„o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi”
2) w art. 1:
   a) ust. 1 otrzymuje brzmienie:
      1. Ustawa określa:
         1) zasady i warunki wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej, organami ścigania państw trzecich, agencjami Unii Europejskiej, organizacjami międzynarodowymi w celu rozpoznawania, wykrywania lub zwalczania przestępstw lub przestępstw skarbowych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego oraz zapobiegania takim przestępstwom i zagrożeniom, a także ścigania sprawców przestępstw lub przestępstw skarbowych;

2) podmioty uprawnione w tych sprawach.

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie: „Podmiotami uprawnionymi do wymiany informacji z podmiotami, o których mowa w ust. 1 pkt 1, są:”

b) w ust. 3 uchyla się pkt 1;

3) w art. 3:

a) pkt 1 otrzymuje brzmienie:

„1) pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, aby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;”,

b) uchyla się pkt 2,

c) pkt 3 otrzymuje brzmienie:

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

d) uchyla się pkt 7,

e) pkt 8 otrzymuje brzmienie:

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

f) dodaje się pkt 9 i 10 w brzmieniu:

„9) organizacji międzynarodowej – rozumie się przez to organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny

organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;

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

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

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

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

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

1) współpracy na terenach przygranicznych, w tym realizowanej przez międzynarodowe centra współpracy;
2) wykonywania zadań oficera łącznikowego podmiotu uprawnionego za granicą lub oficera łącznikowego wchodzącego w skład polskiego biura łącznikowego przy Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol).

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

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

Art. 5. Do zadań punktu kontaktowego należy:

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

5) art. 8 otrzymuje brzmienie:

„Art. 8. 1. Punkt kontaktowy wymienia informacje z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, dostępnymi kanałami komunikacji wykorzystywanymi w międzynarodowej współpracy policyjnej, w szczególności udostępnianymi przez:
1) Międzynarodową Organizację Policji Kryminalnej – Interpol;
2) Agencję Unii Europejskiej ds. Współpracy Organów Ścigania (Europol);
3) biura SIRENE.

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

6) w art. 10 pkt 4 otrzymuje brzmienie:

„4) sposób wymiany informacji między punktem kontaktowym a podmiotami, o których mowa w art. 1 ust. 1 pkt 1, oraz punktem kontaktowym a podmiotami uprawnionymi,";

6) tytuł rozdziału 3 otrzymuje brzmienie:
„Warunki i zasady wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej i agencjami Unii Europejskiej"

7) w art. 11 w ust. 1 pkt 2 otrzymuje brzmienie:
„2) z urzędu przekazują organom ścigania państw członkowskich Unii Europejskiej lub agencjom Unii Europejskiej informacje, jeżeli istnieje uzasadnione przypuszczenie, że informacje te przyczynią się do wykrycia i zatrzymania sprawców przestępstw lub przestępstw skarbowych lub zapobieżenia przestępstwu na terytorium państwa członkowskiego Unii Europejskiej lub państw trzecich, z zastrzeżeniem art. 18d ust. 2.";

8) w art. 12:
a) po ust. 1 dodaje się ust. 1a w brzmieniu:
1a. Podmioty uprawnione, przekazując informacje organom ścigania państw członkowskich Unii Europejskiej, zapewniają, aby wymiana danych osobowych nie była ograniczana ani zakazywana z powodów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.
b) uchyla się ust. 2,
c) dodaje się ust. 3 w brzmieniu:
3. Przekazując informację, podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, wskazują organowi ścigania państwa członkowskiego Unii Europejskiej sposób, w jaki może być ona wykorzystana przez ten organ, w szczególności, czy może być ona wykorzystana w postępowaniu karnym.

10) w art. 16:
a) ust. 1 otrzymuje brzmienie:

1. Podmioty uprawnione przetwarzają informacje uzyskane w wyniku ich wymiany z organami ścigania państw członkowskich Unii Europejskiej w celach wskazanych w art. 1 ust. 1 pkt 1.

b) uchyla się ust. 3;

11) w art. 17 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

2. Jeżeli przy przekazywaniu informacji organ ścigania państwa członkowskiego Unii Europejskiej nie zastrzeże inaczej, informacje uzyskane przez podmiot uprawniony w ten sposób mogą zostać wykorzystane w postępowaniu karnym.

12) po art. 17 dodaje się art. 17a w brzmieniu:

„Art. 17a. Szczegółowe zasady i warunki wymiany informacji z agencjami Unii Europejskiej przez podmioty uprawnione i punkt kontaktowy określają przepisy Unii Europejskiej.";

13) uchyla się art. 18;

14) dodaje się rozdział 3a w brzmieniu:

„Rozdział 3a. Warunki i zasady wymiany informacji z organami ścigania państw trzecich i organizacji międzynarodowych

Art. 18a. 1. Dane osobowe mogą zostać przekazane przez podmioty uprawnione lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, do państwa trzeciego lub organizacji międzynarodowej, jeżeli:

1) przekazanie jest niezbędne do celów, o których mowa w art. 1 ust. 1 pkt 1;
2) dane osobowe są przekazywane administratorowi w państwie trzecim lub organizacji międzynarodowej, który jest podmiotem właściwym do realizacji celów, o których mowa w art. 1 ust. 1 pkt 1, z zastrzeżeniem art. 18e ust. 1;
3) państwo członkowskie Unii Europejskiej, które przekazało dane osobowe, wyraziło uprzednią zgodę na ich przekazanie do państwa trzeciego lub organizacji międzynarodowej, a w przypadku dalszego przekazania tych danych do kolejnego państwa trzeciego lub organizacji międzynarodowej

właściwy organ ścigania, który dokonał pierwotnego przekazania, lub inny właściwy organ ścigania tego samego państwa członkowskiego Unii Europejskiej zezwala na dalsze przekazanie po należytym uwzględnieniu całokształtu sprawy;

4) Komisja Europejska w przypadku, o którym mowa w art. 18b ust. 1, uznała, że państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim, lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych osobowych;
5) w razie braku decyzji Komisji, o której mowa w art. 18b ust. 1:
   a) zostały zapewnione lub istnieją odpowiednie zabezpieczenia zgodnie z art. 18c – w przypadku gdy nie zostały spełnione warunki, o których mowa w pkt 4,
   b) ma zastosowanie wyjątek w szczególnych sytuacjach zgodnie z art. 18d – w przypadku gdy nie zostały spełnione warunki, o których mowa w lit. a.

2. Przekazanie danych osobowych bez uprzedniej zgody innego państwa członkowskiego Unii Europejskiej, o której mowa w ust. 1 pkt 3, jest dozwolone wyłącznie wtedy, gdy takiej uprzedniej zgody nie da się uzyskać w odpowiednim terminie, a przekazanie jest:

1) niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego w państwie członkowskim Unii Europejskiej lub państwie trzecim lub
2) ma istotne znaczenie dla ważnych interesów państwa członkowskiego Unii Europejskiej.

3. W przypadku zastosowania przepisu ust. 2 państwo członkowskie Unii Europejskiej odpowiadające za wydanie uprzedniej zgody zostaje powiadomione o tym bez zbędnej zwłoki.

4. Podmiot uprawniony lub punkt kontaktowy mogą, o ile przepisy odrębne nie stanowią inaczej, zezwolić organowi ścigania państwa członkowskiego Unii Europejskiej na przekazanie do

państwa trzeciego lub organizacji międzynarodowej danych osobowych, uprzednio przekazanych temu organowi przez podmiot uprawniony lub punkt kontaktowy, o ile przekazał on dane osobowe, realizując zadanie określone w art. 5 pkt 1. Jeżeli organ ścigania państwa członkowskiego Unii Europejskiej wystąpił do podmiotu uprawnionego lub punktu kontaktowego o zgodę na dalsze przekazanie danych osobowych uprzednio od nich otrzymanych do kolejnego państwa trzeciego lub organizacji międzynarodowej, organ uprawniony lub punkt kontaktowy może zezwolić na to dalsze przekazanie po należytym uwzględnieniu całokształtu sprawy, w tym:

1) wagi czynu zabronionego;
2) celu, w którym dane osobowe zostały pierwotnie przekazane;
3) stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których dane osobowe są dalej przekazywane.

Art. 18b. 1. Dane osobowe mogą zostać przekazane do państwa trzeciego, terytorium lub przynajmniej jednego sektora w tym państwie trzecim, lub danej organizacji międzynarodowej – o ile Komisja Europejska w drodze decyzji uznała, iż państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub dana organizacja międzynarodowa zapewnia odpowiedni stopień ochrony danych osobowych.

2. Wydanie przez Komisję Europejską decyzji stwierdzającej, że państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony danych osobowych – nie wpływa na przekazywanie danych osobowych do danego państwa trzeciego, terytorium lub jednego lub więcej określonych sektorów w tym państwie trzecim, lub do danej organizacji międzynarodowej na mocy art. 18c i art. 18d.

Art. 18c. 1. W przypadku braku decyzji Komisji Europejskiej, o której mowa w art. 18b ust. 1, dane osobowe mogą zostać

przekazane do państwa trzeciego lub organizacji międzynarodowej, jeżeli przepisy prawa przewidują odpowiednie zabezpieczenia ochrony danych osobowych.
2. W przypadku braku prawnie wiążącego aktu, o którym mowa w ust. 1, dane osobowe mogą zostać przekazane do państwa trzeciego lub organizacji międzynarodowej, jeżeli administrator danych stwierdził, po przeanalizowaniu wszystkich okoliczności związanych z przekazaniem danych osobowych, że to państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni poziom zabezpieczenia ochrony danych osobowych, w szczególności poufności przekazanych danych, celu, w którym dane zostały przekazane, lub sposobu ich wykorzystania, tak aby nie zostały one użyte do wydania orzeczenia lub wykonania kary śmierci, lub innego rodzaju okrutnego lub nieludzkiego traktowania lub karania.
3. Administrator danych dokumentuje fakt przekazania danych osobowych w przypadkach, o których mowa w ust. 2, oraz bez zbędnej zwłoki informuje Prezesa Urzędu Ochrony Danych Osobowych o tym fakcie.
4. Podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, dokumentują, w sposób określony w ust. 5, fakt przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, które zostały przez administratora danych uznane, na podstawie ust. 2, za zapewniające odpowiedni poziom zabezpieczenia ochrony danych osobowych.
5. Podmiot uprawniony lub punkt kontaktowy, o ile realizował zadanie określone w art. 5 pkt 1, udostępnia Prezesowi Urzędu Ochrony Danych Osobowych, na każde jego żądanie, dokumentację obejmującą:
1) datę i godzinę przekazania;
2) informacje o właściwym organie odbierającym;
3) uzasadnienie przekazania;
4) wyliczenie danych osobowych, jakie zostały przekazane.

6. Prezes Urzędu Ochrony Danych Osobowych współpracuje z podmiotami uprawnionymi i punktem kontaktowym w celu prawidłowej realizacji obowiązku zawartego w ust. 2.

Art. 18d. 1. W przypadku braku decyzji Komisji Europejskiej, o której mowa w art. 18b ust. 1, oraz braku odpowiednich zabezpieczeń, o których mowa w art. 18c ust. 1 i 2, dane osobowe lub określona ich kategoria mogą zostać przekazane do państwa trzeciego lub organizacji międzynarodowej wyłącznie pod warunkiem, że przekazanie jest niezbędne:

1) w celu ochrony życia lub zdrowia osoby, której dane dotyczą, lub innej osoby;
2) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą, jeżeli przepisy odrębne tak stanowią;
3) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego Unii Europejskiej lub państwa trzeciego;
4) w indywidualnym przypadku do celów, o których mowa w art. 1 ust. 1 pkt 1;
5) w indywidualnym przypadku dla ustalenia, dochodzenia lub obrony roszczeń w związku z celami określonymi w art. 1 ust. 1 pkt 1.

2. Danych osobowych nie przekazuje się, jeżeli podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, stwierdziły, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem, o którym mowa w ust. 1 pkt 4 i 5.

3. Podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, dokumentują, w sposób określony w ust. 4, fakt przekazania danych osobowych na podstawie ust. 1 do państwa trzeciego lub organizacji międzynarodowej.

4. Podmiot uprawniony lub punkt kontaktowy, o ile realizował zadanie określone w art. 5 pkt 1, udostępnia Prezesowi Urzędu

Ochrony Danych Osobowych, na każde jego żądanie, dokumentację obejmującą:

1) datę i godzinę przekazania;
2) informacje o właściwym organie odbierającym;
3) uzasadnienie przekazania;
4) wyliczenie danych osobowych, jakie zostały przekazane.

Art. 18e. 1. Z zastrzeżeniem wyjątków przewidzianych w umowach międzynarodowych dotyczących współpracy policyjnej zawartych z państwami trzecimi, dane osobowe w indywidualnych i konkretnych przypadkach mogą zostać przekazane bezpośrednio odbiorcom mającym siedzibę w państwach trzecich jedynie wówczas, gdy spełnione zostały łącznie następujące warunki:

1) przekazanie jest niezbędne do wykonania prawnie określonego zadania podmiotu uprawnionego do celów, o których mowa w art. 1 ust. 1 pkt 1;
2) podmiot uprawniony stwierdza, że podstawowe prawa i wolności danej osoby, której dane dotyczą, nie są nadrzędne wobec interesu publicznego przemawiającego za przedmiotowym przekazaniem;
3) podmiot uprawniony uznaje, że przekazanie organowi ścigania państwa trzeciego do celów, o których mowa w art. 1 ust. 1 pkt 1, byłoby nieskuteczne lub niewłaściwe, w szczególności z uwagi na niemożność zachowania odpowiedniego terminu;
4) organ ścigania państwa trzeciego zostaje o tym poinformowany bez zbędnej zwłoki, chyba że byłoby to nieskuteczne lub niewłaściwe;
5) podmiot uprawniony informuje odbiorcę o konkretnym celu, w którym dane osobowe mają być wyłącznie przetwarzane przez odbiorcę, pod warunkiem że takie przetwarzanie jest niezbędne.

2. Podmiot uprawniony lub punkt kontaktowy, o ile realizuje zadanie określone w art. 5 pkt 1, dokumentują fakt przekazania

danych osobowych na podstawie ust. 1 oraz niezwłocznie informują Prezesa Urzędu Ochrony Danych Osobowych o tym fakcie.

3. Podmiot uprawniony lub punkt kontaktowy, o ile realizował zadanie określone w art. 5 pkt 1, udostępnia Prezesowi Urzędu Ochrony Danych Osobowych, na każde jego żądanie, dokumentację obejmującą:

1) datę i godzinę przekazania;
2) informacje o właściwym organie odbierającym;
3) uzasadnienie przekazania;
4) wyliczenie danych osobowych, jakie zostały przekazane.

Art. 18f. Do wymiany informacji z państwami trzecimi lub organizacjami międzynarodowymi stosuje się odpowiednio przepisy art. 11 ust. 1 pkt 2 i ust. 2, art. 12, z wyłączeniem ust. 1a, art. 13, art. 14, art. 16 i art. 17.";

15) art. 19 otrzymuje brzmienie:

„Art. 19. 1. Podmioty uprawnione mogą wymieniać dane osobowe z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, po uprzednim zweryfikowaniu ich prawidłowości, aktualności i kompletności oraz w sposób umożliwiający podmiotom, o których mowa w art. 1 ust. 1 pkt 1, dokonanie oceny tych danych w tym zakresie.

2. Podmiot uprawniony, który otrzymał dane osobowe od podmiotów, o których mowa w art. 1 ust. 1 pkt 1, bez wniosku, dokonuje niezwłocznie weryfikacji tych danych w zakresie ich przydatności do realizacji celu, w którym dane zostały przekazane.

3. Podmiot uprawniony lub punkt kontaktowy, który przekazał nieprawdziwe, niekompletne, nieaktualne lub niezupełne dane osobowe albo przekazał te dane z naruszeniem przepisów ustawy, jest obowiązany, bez zbędnej zwłoki, poinformować o tym podmioty, o których mowa w art. 1 ust. 1 pkt 1, oraz sprostować, uzupełnić lub uaktualnić te dane, przekazując dane właściwe, albo, w zależności od okoliczności, o których mowa w art. 21 ust. 1, dane te usunąć.

16) w art. 20:

a) ust. 1 i 2 otrzymują brzmienie:
1. Dane osobowe, uzyskane w wyniku wymiany z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, podmiot uprawniony przechowuje przez okres niezbędny do realizacji celu, w jakim te dane zostały uzyskane, lub przez okres niezbędny do wykrywania i ścigania sprawców przestępstw lub przestępstw skarbowych oraz zapobiegania przestępczości lub jej zwalczania, zgodnie z terminami oraz zasadami przetwarzania danych w zbiorach danych administrowanych przez dany podmiot uprawniony.
2. Podmioty uprawnione dokonują weryfikacji zgromadzonych danych osobowych i usuwają dane zbędne albo dokonują ich pseudonimizacji.
b) uchyla się ust. 3 i 4,
c) dodaje się ust. 5 w brzmieniu:
5. Dane osobowe, wymieniane z podmiotami, o których mowa w art. 1 ust. 1 pkt 1, oraz podmiotami uprawnionymi, punkt kontaktowy przechowuje i przetwarza przez okres niezbędny do realizacji zadania, o którym mowa w art. 5 pkt 5.

17) w art. 21 ust. 1 otrzymuje brzmienie:
1. Jeżeli podmiot, o którym mowa w art. 1 ust. 1 pkt 1, przy wymianie danych osobowych określił termin ich przechowywania, po upływie którego wymagane jest ich usunięcie lub zweryfikowanie, podmiot uprawniony, który te dane otrzymał i przechowuje, ma obowiązek zachowania takiego terminu.

18) art. 22 otrzymuje brzmienie:
„Art. 22. Jeżeli podmiot, o którym mowa w art. 1 ust. 1 pkt 1, przy wymianie danych osobowych określił ograniczenia dotyczące przetwarzania tych danych wynikające z prawa krajowego tego państwa, podmiot uprawniony, który te dane otrzymał i przechowuje, ma obowiązek uwzględnić takie ograniczenia.";

19) w art. 23 ust. 1 otrzymuje brzmienie:
1. Podmioty uprawnione, które przekazały lub udostępniły dane osobowe podmiotowi, o którym mowa w art. 1 ust. 1 pkt 1, albo

otrzymały takie dane od tego podmiotu, odnotowują lub dokumentują fakt takiego przekazania, udostępnienia lub otrzymania w celu weryfikacji legalności przetwarzanych danych, ich integralności oraz zapewnienia ich bezpieczeństwa.

20) uchyla się art. 24 i art. 25;

21) art. 26 otrzymuje brzmienie:

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

Artykuł 86. Zmiany w ustawie o zużytym sprzęcie elektrycznym i elektronicznym.

W ustawie z dnia 11 września 2015 r. o zużytym sprzęcie elektrycznym i elektronicznym (Dz.U. z 2018 r. poz. 1466 i 1479) w art. 2 w ust. 2 w pkt 10 kropkę zastępuje się średnikiem i dodaje się pkt 11 w brzmieniu:

„11) informatycznych nośników danych wykorzystywanych do przetwarzania danych osobowych, o których mowa w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125).”.

Artykuł 87. Zmiany w ustawie Prawo o prokuraturze.

W ustawie z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz.U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5, 1000, 1443 i 1669) po art. 191 dodaje się art. 191a w brzmieniu:

„Art. 191a. § 1. Nadzór nad przetwarzaniem danych osobowych w ramach realizacji zadań określonych w art. 2, których administratorami są powszechne jednostki organizacyjne prokuratury

zgodnie z art. 13 § 6, wykonują w zakresie działalności prokuratury:
1) rejonowej – prokurator okręgowy;
2) okręgowej – prokurator regionalny;
3) regionalnej i Prokuratury Krajowej – Prokurator Krajowy.

§ 2. W ramach nadzoru, o którym mowa w § 1, właściwe organy:
1) rozpatrują skargi osób, których dane osobowe są przetwarzane niezgodnie z prawem;
2) podejmują działania mające na celu upowszechnianie wśród nadzorowanych administratorów danych i podmiotów przetwarzających wiedzy o obowiązkach wynikających z ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125);
3) współpracują wzajemnie oraz z organami sprawującymi nadzór nad przetwarzaniem danych osobowych w ramach postępowań prowadzonych przez sądy i trybunały z organami nadzorczymi w rozumieniu art. 51 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[24)]), jak też współpracują między sobą, w tym dzielą się informacjami, oraz świadczą z tymi organami i między sobą wzajemną pomoc w celu zapewnienia spójnego stosowania przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

§ 3. Organy, o których mowa w § 1, są uprawnione do:
1) nakazywania administratorowi lub podmiotowi przetwarzającemu albo ich przedstawicielom dostarczenia wszelkich informacji potrzebnych do realizacji zadań tego organu;

2) zawiadamiania administratora danych lub podmiotu przetwarzającego o podejrzeniu naruszenia przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
3) uzyskiwania od administratora danych i podmiotu przetwarzającego dostępu do wszelkich danych osobowych oraz informacji niezbędnych organowi nadzorczemu do realizacji jego zadań;
4) uzyskiwania dostępu do pomieszczeń administratora danych i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych;
5) wydawania ostrzeżeń administratorowi danych lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
6) udzielania upomnień administratorowi danych lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
7) wzywania administratora danych lub podmiotu przetwarzającego do dostosowania operacji przetwarzania danych do przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

§ 4. Do przyjmowania i rozpatrywania skarg, o których mowa w § 2 pkt 1, stosuje się odpowiednio przepisy działu VI.

Artykuł 88. Zmiany w ustawie o bezpieczeństwie obrotu prekursorami materiałów wybuchowych.

W ustawie z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (Dz.U. z 2018 r. poz. 410 i 1000) art. 9 otrzymuje brzmienie:

„Art. 9. Do danych osobowych zgromadzonych w systemie zgłaszania stosuje się przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125).”.

Artykuł 89. Zmiany w ustawie o Krajowej Administracji Skarbowej.

W ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz.U. z 2018 r. poz. 508, z późn. zm.[25)]) wprowadza się następujące zmiany:

1) w art. 35 dodaje się ust. 5 w brzmieniu:
   5. Do danych zgromadzonych oraz przetwarzanych w CRDP w związku z realizacją zadań związanych z rozpoznawaniem, zapobieganiem, wykrywaniem i zwalczaniem czynów zabronionych stosuje się przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125).
2) po art. 47 dodaje się art. 47a w brzmieniu:
   „Art. 47a. Organy KAS w celu realizacji ustawowych zadań są uprawnione do wymiany informacji, w tym danych osobowych, z organami ścigania państw członkowskich Unii Europejskiej zajmującymi się zapobieganiem i zwalczaniem przestępczości oraz innymi organizacjami międzynarodowymi na zasadach i warun-

kach określonych w przepisach odrębnych, prawie Unii Europejskiej i umowach międzynarodowych.";

2) po art. 52 dodaje się art. 52a–52c w brzmieniu:

„Art. 52a. 1. Przetwarzanie danych osobowych przez organy KAS w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, odbywa się na zasadach określonych w tej ustawie.

2. Danych osobowych, o których mowa w art. 14 ust. 1 ustawy, o której mowa w ust. 1, nie gromadzi się, w przypadku gdy nie mają one przydatności wykrywczej lub dowodowej.

Art. 52b. 1. Dane osobowe zbierane i przetwarzane przez KAS na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[26)]) mogą być przetwarzane przez organy KAS również dla celów określonych w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

2. Dane osobowe przetwarzane przez KAS dla celów określonych w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości mogą być przetwarzane przez organy KAS również dla innych celów.

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

3) po art. 126 dodaje się art. 126a w brzmieniu:

„Art. 126a. Przetwarzanie danych osobowych na podstawie niniejszej ustawy przez właściwe organy KAS w celu realizowania zadań oraz wykonywania czynności, o których mowa w art. 113 ust. 1, odbywa się na zasadach określonych w ustawie z dnia

14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, prawie Unii Europejskiej oraz postanowieniach umów międzynarodowych.”.

Artykuł 90. Zmiany w ustawie o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym.

W ustawie z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz.U. poz. 2072) po art. 35 dodaje się art. 35a i art. 35b w brzmieniu:

„Art. 35a. 1. Trybunał jest administratorem danych osobowych przetwarzanych w ramach prowadzonych przez niego postępowań.

2. Do przetwarzania danych osobowych w postępowaniach prowadzonych przez Trybunał przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[27)]), zwanego dalej ”rozporządzeniem 2016/679”, nie stosuje się.

3. W związku z przetwarzaniem danych osobowych w postępowaniach prowadzonych przez Trybunał wykonanie obowiązków, o których mowa w art. 13 rozporządzenia 2016/679, następuje przez umieszczenie informacji określonych w art. 13 ust. 2 rozporządzenia 2016/679 w Biuletynie Informacji Publicznej na stronie podmiotowej oraz w widocznym miejscu w budynku Trybunału.

Art. 35b. 1. Nadzór nad przetwarzaniem danych osobowych przez Trybunał w ramach prowadzonych przez niego postępowań wykonuje Krajowa Rada Sądownictwa.
2. Do nadzoru, o którym mowa w ust. 1, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych stosuje się odpowiednio."

Artykuł 91. Zmiany w ustawie o wymianie informacji podatkowych z innymi państwami.

W ustawie z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami (Dz.U. poz. 648 oraz z 2018 r. poz. 723, 1499 i 2193) po art. 6 dodaje się art. 6a w brzmieniu:

„Art. 6a. Do udostępniania informacji otrzymanych na podstawie ustawy oraz umów o unikaniu podwójnego opodatkowania, innych ratyfikowanych umów, których stroną jest Rzeczpospolita Polska, oraz innych umów międzynarodowych, których stroną jest Unia Europejska, a także porozumień zawartych na podstawie tych umów, nie stosuje się przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125) w zakresie, w jakim jest to niezgodne z postanowieniami tych umów lub porozumień lub przepisami ustawy.".

Artykuł 92. Zmiany w ustawie Prawo wodne.

W ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz.U. z 2018 r. poz. 2268) po art. 341 dodaje się art. 341a w brzmieniu:

„Art. 341a. Administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związ-

ku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), jest minister właściwy do spraw gospodarki wodnej lub organ wykonujący kontrolę.”.

Artykuł 93. Zmiany w ustawie o Sądzie Najwyższym.

W ustawie z dnia 8 grudnia 2017 r. o Sądzie Najwyższym (Dz.U. z 2018 r. poz. 5, z późn. zm.[28)]) wprowadza się następujące zmiany:

1) art. 8 otrzymuje brzmienie:
„Art. 8. Sąd Najwyższy niezwłocznie publikuje wydane przez siebie orzeczenie, a po sporządzeniu jego uzasadnienia – również uzasadnienie orzeczenia, w Biuletynie Informacji Publicznej na stronie podmiotowej Sądu Najwyższego.”;
2) po art. 9 dodaje się art. 9a w brzmieniu:
„Art. 9a. § 1. Sąd Najwyższy jest administratorem danych osobowych przetwarzanych w postępowaniach sądowych.
§ 2. Do przetwarzania danych osobowych w postępowaniach sądowych przepisów art. 15, art. 16 – w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania, oraz art. 18 i art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[29)]), zwanego dalej ”rozporządzeniem 2016/679”, nie stosuje się.
§ 3. W związku z przetwarzaniem danych osobowych w postępowaniach sądowych wykonanie obowiązków, o których mowa w art. 13 rozporządzenia 2016/679, następuje przez umieszczenie informacji określonych w art. 13 ust. 2 rozporządzenia 2016/679 w Biuletynie Informacji Publicznej na stronie podmiotowej oraz w widocznym miejscu w budynku Sądu Najwyższego.

3) po art. 97 dodaje się art. 97a w brzmieniu:
„Art. 97a. § 1. Nadzór nad przetwarzaniem danych osobowych w postępowaniach sądowych wykonuje Krajowa Rada Sądownictwa.
§ 2. Do nadzoru, o którym mowa w § 1, przepisy art. 175dd § 2 i 3 oraz działu I rozdziału 5a ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych stosuje się odpowiednio."

Artykuł 94. Zmiany w ustawie o Służbie Ochrony Państwa.

W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz.U. z 2018 r. poz. 138, z późn. zm.[30)]) wprowadza się następujące zmiany:

1) w art. 3 w pkt 3 po wyrazach "funkcjonariuszy i pracowników" dodaje się wyraz "SOP,";
2) w art. 6 w ust. 2 pkt 1 otrzymuje brzmienie:
„1) przekazują SOP wszelkie informacje, w tym dane osobowe, mogące mieć wpływ na bezpieczeństwo ochranianych osób lub obiektów;";
3) w art. 51 skreśla się zdanie drugie;
4) w art. 56:
a) w ust. 6 pkt 1 otrzymuje brzmienie:
„1) dane osobowe, o których mowa w art. 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125);",
b) w ust. 8 wprowadzenie do wyliczenia otrzymuje brzmienie:
„Dane osobowe, o których mowa w ust. 2 i 3 oraz art. 40 ust. 1, z wyjątkiem danych osobowych, o których mowa w ust. 6 pkt 1, SOP może przetwarzać:"
c) uchyla się ust. 9 i 11;

5) w art. 59 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie: „W celu realizacji zadań, o których mowa w art. 19 ust. 1 pkt 2, SOP może uzyskiwać dane:"
6) uchyla się art. 60;
7) art. 61 otrzymuje brzmienie:
„Art. 61. Administratorem danych osobowych przetwarzanych przez SOP jest Komendant SOP.";
8) po art. 70 dodaje się art. 70a w brzmieniu:
„Art. 70a. 1. SOP jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w SOP, przenoszenia do służby w SOP oraz w zakresie wynikającym z przebiegu stosunku służbowego funkcjonariuszy SOP, także po jego ustaniu, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[31)]), zwanego dalej "rozporządzeniem (UE) 2016/679", z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.
2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych osobowych po pisemnym zobowiązaniu funkcjonariuszy lub pracowników do zachowania przetwarzanych danych w poufności."

Artykuł 95. Zmiany w ustawie o Straży Marszałkowskiej.

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

1) w art. 3 dodaje się ust. 6–8 w brzmieniu:
„6. Do pracowników Straży Marszałkowskiej, o których mowa w ust. 5, stosuje się odpowiednio przepisy art. 21 ust. 1, 2, 4, art. 22 ust. 1, art. 23 ust. 1, art. 24, art. 27–29, art. 30 ust. 1a–3 oraz art. 48 ust. 1a pkt 3 oraz ust. 1b i 1c ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz.U. z 2018 r. poz. 1915).
7. Uprawnienia kierowników urzędów przewidziane w art. 48 ust. 1a pkt 3 oraz ust. 1b i 1c ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych w odniesieniu do pracowników Straży Marszałkowskiej, o których mowa w ust. 5, wykonuje Komendant Straży Marszałkowskiej.
8. Regulamin wynagradzania pracowników Straży Marszałkowskiej, o których mowa w ust. 5, zatwierdza Marszałek Sejmu."
2) w art. 4:
   a) po ust. 2 dodaje się ust. 2a w brzmieniu:
   „2a. Administratorem danych osobowych, o których mowa w ust. 2 pkt 2, jest Komendant Straży Marszałkowskiej."
   c) uchyla się ust. 4;
2) po art. 19 dodaje się art. 19a w brzmieniu:
„Art. 19a. 1. Straż Marszałkowska jest uprawniona do przetwarzania informacji, w tym danych osobowych, w zakresie niezbędnym do prowadzenia postępowań kwalifikacyjnych do służby w Straży Marszałkowskiej, przenoszenia do służby w Straży Marszałkowskiej oraz w zakresie wynikającym z przebiegu stosunku służbowego funkcjonariuszy Straży Marszałkowskiej, także po jego ustaniu, w tym ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[32)]), zwanego dalej "rozporządzeniem (UE) 2016/679", z wyłączeniem danych dotyczących kodu genetycznego oraz danych daktyloskopijnych.

2. Do przetwarzania danych osobowych, o których mowa w ust. 1, nie stosuje się art. 13 ust. 1 lit. d i e oraz art. 16 rozporządzenia (UE) 2016/679 w zakresie, w jakim przepisy szczególne przewidują odrębny tryb sprostowania. Zabezpieczenie przetwarzania danych osobowych polega co najmniej na dopuszczeniu do ich przetwarzania wyłącznie funkcjonariuszy Straży Marszałkowskiej lub pracowników posiadających pisemne upoważnienie wydane przez administratora danych po pisemnym zobowiązaniu funkcjonariuszy Straży Marszałkowskiej lub pracowników do zachowania przetwarzanych danych w poufności."

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

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

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

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

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

Artykuł 96. Zmiany w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

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

1) w art. 96 ust. 3 otrzymuje brzmienie:
   „3. Dane, o których mowa w art. 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), mogą być zbierane i wykorzystywane oraz przetwarzane przez Generalnego Inspektora wyłącznie w przypadku, gdy jest to niezbędne ze względu na zakres wykonywanych zadań lub czynności."
2) w art. 97:
   a) uchyla się ust. 1–5,
   b) ust. 6 i 7 otrzymują brzmienie:
      „6. Kierownik komórki organizacyjnej, o której mowa w art. 12 ust. 2, któremu inspektor ochrony danych wydał pisemne polecenie usunięcia stwierdzonych uchybień, informuje Generalnego Inspektora, w terminie 7 dni od dnia wydania tego polecenia, o jego wykonaniu lub przyczynie jego niewykonania.
      7. W przypadku naruszenia przepisów ustawy lub przepisów o ochronie danych osobowych inspektor ochrony danych podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Generalnego Inspektora oraz ministra właściwego do spraw finansów publicznych."
3) uchyla się ust. 8.

Artykuł 97. Zmiany w ustawie o przetwarzaniu danych dotyczących przelotu pasażera.

W ustawie z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. poz. 894) wprowadza się następujące zmiany:

1) w art. 9 w ust. 2 pkt 5 otrzymuje brzmienie:
   „5) pouczenie o prawie do złożenia wniosku o udzielenie informacji o przysługujących mu prawach lub złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych w zakresie przetwarzania danych osobowych pasażera w związku z przetwarzaniem danych PNR.";
2) w art. 36 po pkt 4 dodaje się pkt 4a w brzmieniu:
   „4a) Komendant Służby Ochrony Państwa;";
3) w art. 53:
   a) w ust. 1 pkt 3 otrzymuje brzmienie:
      „3) państwo trzecie zapewnia odpowiedni poziom ochrony przekazywanych danych określony w art. 18b–18d ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2018 r. poz. 484 oraz z 2019 r. poz. 125);",
   b) uchyla się ust. 2;
4) w art. 59 w ust. 1 pkt 2 otrzymuje brzmienie:
   „2) sprawuje nadzór nad zgodnością przetwarzania danych PNR przez JIP z przepisami niniejszej ustawy oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125);";
5) w art. 62 w ust. 3 pkt 2 otrzymuje brzmienie:
   „2) sprawdza zgodność przetwarzania danych PNR z prawem, prowadzi postępowania i wykonuje inne czynności, zgodnie

z ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, z własnej inicjatywy lub na podstawie zażalenia osoby, której dane PNR są przetwarzane.";

6) w art. 63 ust. 3 otrzymuje brzmienie:
„3. Kontrola, o której mowa w ust. 1, jest sprawowana zgodnie z przepisami ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

7) użyte w art. 59 w ust. 1 w pkt 3 i w ust. 2 w pkt 4 i 5, w art. 61, w art. 62 oraz w art. 63 w ust. 1 i 2, w różnym przypadku wyrazy "Generalny Inspektor Ochrony Danych Osobowych" zastępuje się użytymi w odpowiednim przypadku wyrazami "Prezes Urzędu Ochrony Danych Osobowych".

Rozdział 10. Przepisy przejściowe, dostosowujące i końcowe.

Artykuł 98. Pełnienie funkcji inspektora ochrony danych.

1. Osoba pełniąca w dniu wejścia w życie niniejszej ustawy funkcję inspektora ochrony danych osobowych na podstawie przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 i 1669), staje się inspektorem ochrony danych i pełni swoją funkcję nie dłużej jednak niż 3 miesiące od dnia wejścia w życie niniejszej ustawy, chyba że przed tym dniem administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na inspektora ochrony danych, w sposób określony w art. 46.

2. Osoba, która stała się inspektorem ochrony danych na podstawie ust. 1, pełni swoją funkcję także po upływie 3 miesięcy od dnia wejścia w życie niniejszej ustawy, jeżeli do tego dnia administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o jej wyznaczeniu, w sposób określony w art. 46.

3. Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał inspektora ochrony danych osobowych, o którym mowa w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, jest obowiązany do wyznaczenia inspektora ochrony danych i zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu, w terminie 1 miesiąca od dnia wejścia w życie niniejszej ustawy.

Artykuł 99. Kontrole w toku.

1. Do kontroli wszczętych na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723) i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

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

Artykuł 100. Prowadzenie postępowań na podstawie przepisów dotychczasowych.

1. Postępowania prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych, wszczęte i niezakończone przed dniem wejścia w życie niniejszej ustawy, prowadzone są na podstawie przepisów dotychczasowych.

2. Czynności dokonane w postępowaniach, o których mowa w ust. 1, pozostają skuteczne, o ile zostały dokonane zgodnie z przepisami obowiązującymi w czasie ich dokonywania.

3. W przypadku wniesienia przed dniem wejścia w życie niniejszej ustawy, na podstawie art. 21 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wniosku o ponowne rozpatrzenie sprawy, będące w toku postępowanie wszczęte tym wnioskiem umarza się z mocy prawa z dniem wejścia w życie niniejszej ustawy.

4. Stronę, która zainicjowała postępowanie, o którym mowa w ust. 3, organ poucza o prawie złożenia do sądu administracyjnego skargi na decyzję, od której strona złożyła wniosek o ponowne rozpatrzenie sprawy.

5. Termin na wniesienie skargi w przypadku, o którym mowa w ust. 4, wynosi 3 miesiące od dnia doręczenia pouczenia. Do czasu upływu tego terminu decyzja, od której strona złożyła wniosek o ponowne rozpatrzenie sprawy, nie podlega wykonaniu.

Artykuł 101. Termin odpowiedzi na wystąpienie lub wniosek.

Podmiot, do którego przed dniem wejścia w życie niniejszej ustawy zostało skierowane wystąpienie lub wniosek, o których mowa w art. 19a ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jest obowiązany przekazać Prezesowi Urzędu Ochrony Danych Osobowych odpowiedź na wystąpienie lub wniosek, na piśmie, w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

Artykuł 102. Termin dostosowania zasad przetwarzania danych do środków technicznych i organizacyjnych.

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

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

3. Dotychczasowe rozstrzygnięcia określające zasady udostępniania informacji i danych osobowych z Centralnej Bazy Danych Osób Pozbawionych Wolności, za pośrednictwem systemu teleinformatycznego, zachowują moc do dnia wejścia w życie decyzji wydanych na podstawie art. 25d ust. 1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, nie dłużej jednak niż przez okres 2 lat od dnia wejścia w życie niniejszej ustawy.

4. Dostosowanie zasad przetwarzania informacji i danych osobowych w zbiorach danych utworzonych przed dniem wejścia w życie niniejszej ustawy do wymogów, o których mowa w art. 19, art. 20 i art. 36, nastąpi nie później niż do dnia 6 maja 2023 r.

Artykuł 103. Obowiązywanie upoważnień do przetwarzania danych osobowych.

Wydane przed dniem wejścia w życie ustawy upoważnienia do przetwarzania danych osobowych zachowują moc przez okres 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Artykuł 104. Zgody zachowane w mocy.

Zgody wydane przez służby, instytucje państwowe oraz organy władzy publicznej na udostępnianie za pomocą urządzeń telekomunikacyjnych lub w drodze teletransmisji informacji, w tym danych osobowych, jednostkom organizacyjnym Policji, jednostkom organizacyjnym Straży Granicznej, Służbie Ochrony Państwa oraz organom Krajowej Administracji Skarbowej zachowują swoją moc, z zastrzeżeniem art. 102 ust. 3.

Artykuł 105. Obowiązywanie przepisów wykonawczych.

Dotychczasowe przepisy wykonawcze wydane na podstawie:
1) art. 15 ust. 8 i art. 20 ust. 19 ustawy zmienianej w art. 58,
2) art. 10a ust. 8 i art. 11 ust. 2 ustawy zmienianej w art. 59,
3) art. 25 ust. 3 ustawy zmienianej w art. 80,
4) art. 29 ust. 8 ustawy zmienianej w art. 72,
5) art. 42 ust. 6 ustawy zmienianej w art. 81,
6) art. 10 ustawy zmienianej w art. 85

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

1) art. 15 ust. 8, art. 20 ust. 1n i art. 20 ust. 1o ustawy zmienianej w art. 58, w brzmieniu nadanym niniejszą ustawą,
2) art. 10a ust. 18 i art. 11 ust. 2 ustawy zmienianej w art. 59, w brzmieniu nadanym niniejszą ustawą,
3) art. 25 ust. 3 ustawy zmienianej w art. 80, w brzmieniu nadanym niniejszą ustawą,
4) art. 29 ust. 17 ustawy zmienianej w art. 72, w brzmieniu nadanym niniejszą ustawą,
5) art. 42 ust. 6 ustawy zmienianej w art. 81, w brzmieniu nadanym niniejszą ustawą,
6) art. 10 ustawy zmienianej w art. 85, w brzmieniu nadanym niniejszą ustawą

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

Artykuł 106. Limit wydatków z budżetu państwa.

1. Maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy wynosi w:
1) 2019 r. – 1 250 000 zł;
2) 2020 r. – 1 350 000 zł;

3) 2021 r. – 1 380 000 zł;
4) 2022 r. – 1 410 000 zł;
5) 2023 r. – 1 450 000 zł;
6) 2024 r. – 1 490 000 zł;
7) 2025 r. – 1 530 000 zł;
8) 2026 r. – 1 570 000 zł;
9) 2027 r. – 1 610 000 zł;
10) 2028 r. – 1 650 000 zł.

2. Prezes Urzędu Ochrony Danych Osobowych monitoruje wykorzystanie limitu wydatków, o których mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału. Ocena za IV kwartał jest dokonywana według stanu na dzień 20 listopada danego roku.

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

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

Artykuł 107. Uchylenie zachowanych w mocy przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Tracą moc art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziały 4, 5 i 7 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych zachowane w mocy w odnie-

sieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119 z 04.05.2016, str. 89) na podstawie art. 175 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Artykuł 108. Wejście w życie.

Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:

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

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680

z dnia 27 kwietnia 2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW)

Rozdział I. Przepisy ogólne

Artykuł 1. Przedmiot i cele.

1. Niniejsza dyrektywa ustanawia przepisy o ochronie 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 tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

2. Zgodnie z niniejszą dyrektywą państwa członkowskie:

a) chronią prawa podstawowe i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych; oraz

b) zapewniają, by wymiana danych osobowych przez właściwe organy w Unii, jeżeli wynika z prawa Unii lub prawa krajowego, nie była ograniczana ani zakazywana z powodów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

3. Niniejsza dyrektywa nie wyklucza ustanowienia przez państwa członkowskie zabezpieczeń wyższych niż zabezpieczenia przewidziane w niniejszej dyrektywie dla ochrony praw i wolności osoby, której dane dotyczą, w związku z przetwarzaniem danych osobowych przez właściwe organy.

Artykuł 2. Zakres zastosowania.

1. Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów określonych w art. 1 ust. 1.

2. Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany, oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

3. Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;
b) przez instytucje, organy i jednostki organizacyjne Unii.

Artykuł 3. Definicje.

Na użytek niniejszej dyrektywy:

1) „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania oso-

ba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2) „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
3) „ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
4) „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
5) „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6) „zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7) „właściwy organ" oznacza:
   a) organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; lub
   b) inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;
8) „administrator" oznacza właściwy organ, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby przetwarzania są określone prawem Unii lub prawem państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
9) „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
10) „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być

zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

11) „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
12) „dane genetyczne" oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
13) „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, takie jak wizerunek twarzy lub dane daktyloskopijne;
14) „dane dotyczące zdrowia" oznaczają dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia;
15) „organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie na mocy art. 41;
16) „organizacja międzynarodowa" oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

Rozdział II. Zasady

Artykuł 4. Zasady dotyczące przetwarzania danych osobowych.

1. Państwa członkowskie zapewniają, by dane osobowe były:

a) przetwarzane zgodnie z prawem i rzetelnie;
b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami;
c) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe, w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2. Przetwarzanie przez tego samego lub innego administratora w jednym z celów określonych w art. 1 ust. 1 innym niż cel, w którym dane osobowe zostały zebrane, jest dozwolone, o ile:

a) administratorowi wolno przetwarzać takie dane osobowe w takim celu na mocy prawa Unii lub prawa państwa członkowskiego; oraz
b) przetwarzanie jest niezbędne i proporcjonalne w tym innym celu na mocy prawa Unii lub prawa państwa członkowskiego.

3. Przetwarzanie przez tego samego lub innego administratora może obejmować archiwizację w interesie publicznym, wykorzystanie do celów naukowych, statystycznych lub historycznych, o których mowa w art. 1 ust. 1, o ile podlega ono odpowiednim zabezpieczeniom praw i wolności osób, których dane dotyczą.

4. Za przestrzeganie przepisów ust. 1, 2 i 3 odpowiada administrator, który musi być w stanie wykazać fakt ich przestrzegania.

Artykuł 5. Terminy przechowywania i przeglądu

Państwa członkowskie zapewniają, by przyjęto odpowiednie terminy usuwania danych osobowych lub okresowego przeglądu konieczności przechowywania danych osobowych. Przestrzeganiu tych terminów służą odpowiednie środki proceduralne.

Artykuł 6. Rozróżnianie poszczególnych kategorii osób, których dane dotyczą

Państwa członkowskie zapewniają, by administrator – w stosownym przypadku i w miarę możliwości – wyraźnie rozróżniał dane osobowe poszczególnych kategorii osób, których dane dotyczą, takich jak:

a) osoby, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
b) osoby skazane za czyn zabroniony;
c) pokrzywdzeni czynem zabronionym lub osoby, w przypadku których określone fakty wskazują, że mogą stać się ofiarą czynu zabronionego; oraz
d) osoby inne w stosunku do czynu zabronionego, takie jak osoby, które mogą zostać wezwane do złożenia zeznań w ramach postępowania przygotowawczego w sprawie czynu zabronionego lub

na dalszych etapach postępowania karnego, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w lit. a) i b).

Artykuł 7. Rozróżnianie pomiędzy danymi osobowymi i weryfikacja jakości danych osobowych

1. Państwa członkowskie zapewniają, by dane osobowe oparte na faktach były rozróżniane, tak dalece, jak to możliwe, z danymi osobowych opartymi na indywidualnych ocenach.

2. Państwa członkowskie zapewniają, by właściwe organy podejmowały wszelkie rozsądne działania dla zagwarantowania, by nieprawidłowe, niekompletne lub nieaktualne dane osobowe nie były przesyłane lub udostępniane. W tym celu każdy właściwy organ weryfikuje tak dalece, jak to zasadne, jakość danych osobowych przed ich przesłaniem lub udostępnieniem. W miarę możliwości, we wszystkich przypadkach przesyłania danych osobowych, należy dodać niezbędne dodatkowe informacje pozwalające właściwemu organowi odbierającemu ocenić stopień prawidłowości, kompletności i wiarygodności danych osobowych oraz stopień ich aktualności.

3. Jeżeli okaże się, że przesłano dane nieprawidłowe, lub że dane osobowe przesłano niezgodnie z prawem, należy o tym bezzwłocznie powiadomić odbiorcę. W takim przypadku dane osobowe należy sprostować, usunąć lub ograniczyć ich przetwarzanie zgodnie z art. 16.

Artykuł 8. Zgodność przetwarzania z prawem

1. Państwa członkowskie zapewniają, by przetwarzanie było zgodne z prawem wyłącznie wówczas i w zakresie, w jakim jest ono niezbędne do wykonania zadania realizowanego przez właściwy

organ w celach określonych w art. 1 ust. 1 oraz ma podstawę w prawie Unii lub prawie państwa członkowskiego.

2. Prawo państwa członkowskiego regulujące przetwarzanie w zakresie stosowania niniejszej dyrektywy określa co najmniej powody przetwarzania, dane osobowe mające podlegać przetwarzaniu oraz cele przetwarzania.

Artykuł 9. Szczególne warunki przetwarzania

1. Danych osobowych zebranych przez właściwe organy do celów określonych w art. 1 ust. 1 nie przetwarza się do celów innych niż określone w art. 1 ust. 1, chyba że takie przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego. Jeżeli przetwarzanie danych osobowych odbywa się w takich innych celach, zastosowanie ma rozporządzenie (UE) 2016/679, chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii.

2. Jeżeli prawo państwa członkowskiego powierza właściwym organom wykonywanie zadań innych niż zadania wykonywane w celach określonych w art. 1 ust. 1, to do przetwarzania w takich celach, w tym na potrzeby archiwizacji w interesie publicznym, wykorzystania do celów naukowych, statystycznych lub historycznych, ma zastosowanie rozporządzenie (UE) 2016/679, chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii.

3. Państwa członkowskie zapewniają, by wówczas, gdy prawo Unii lub państwa członkowskiego mające zastosowanie do właściwego organu przesyłającego przewiduje szczególne warunki przetwarzania, właściwy organ przesyłający informował odbiorcę takich danych osobowych o tych warunkach i o obowiązku ich przestrzegania.

4. Państwa członkowskie zapewniają, by właściwy organ przesyłający nie stosował warunków wskazanych w ust. 3 do odbiorców w innych państwach członkowskich ani w organach i jednostkach

organizacyjnych ustanowionych na mocy tytułu V rozdział 4 i 5 TFUE, innych niż mające zastosowanie do podobnego przesyłania danych w obrębie państwa członkowskiego właściwego organu przesyłającego.

Artykuł 10. Przetwarzanie szczególnych kategorii danych osobowych

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 jest dozwolone wyłącznie wtedy, jeżeli jest bezwzględnie niezbędne, podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, oraz:

a) jest dopuszczone prawem Unii lub prawem państwa członkowskiego;
b) jest niezbędne dla ochrony żywotnych interesów osoby fizycznej, której dane dotyczą, lub innej osoby; lub
c) takie przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

Artykuł 11. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

1. Państwa członkowskie zapewniają, by decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i mają niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływają, były zakazane, chyba że dopuszcza je prawo Unii lub prawo państwa członkowskiego, które-

mu podlega administrator i które przewiduje odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora.

2. Decyzje, o których mowa w ust. 1 niniejszego artykułu, nie mogą opierać się na danych osobowych szczególnych kategorii, o których mowa w art. 10, chyba że istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.

3. Profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii, o których mowa w art. 10, jest zabronione zgodnie z prawem Unii.

Rozdział III. Prawa osoby, której dane dotyczą

Artykuł 12. Komunikacja oraz ułatwienia w wykonywaniu praw osób, których dane dotyczą

1. Państwa członkowskie zapewniają, by administrator podejmował wszelkie rozsądne działania, aby udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13, oraz aby prowadził z nią wszelką komunikację wskazaną w art. 11, 14–18 i 31 w sprawie przetwarzania w zwięzłej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka. Informacji udziela się wszelkimi stosownymi sposobami, w tym elektronicznie. Co do zasady administrator udziela informacji w takiej samej formie, w jakiej wniesiono żądanie.

2. Państwa członkowskie zapewniają, by administrator ułatwiał osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy art. 11 i 14–18.

3. Państwa członkowskie zapewniają, by administrator bez zbędnej zwłoki informował pisemnie osobę, której dane dotyczą, o działaniach podjętych w związku z jej żądaniem.

4. Państwa członkowskie zapewniają, by informacje przekazywane na mocy art. 13 oraz wszelka komunikacja i wszelkie działania podjęte na mocy art. 11, 14–18 i 31 były wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są w sposób oczywisty nieuzasadnione lub nadmierne, zwłaszcza ze względu na ich powtarzalność, administrator może:

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

Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na administratorze.

5. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 14 i 16, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Artykuł 13. Informacje udostępniane lub przekazywane osobie, której dane dotyczą

1. Państwa członkowskie zapewniają, by administrator udostępniał osobie, której dane dotyczą, przynajmniej następujące informacje:

a) tożsamość i dane kontaktowe administratora;
b) dane kontaktowe inspektora ochrony danych, w razie potrzeby;
c) cele przetwarzania, do których mają posłużyć dane osobowe;
d) informacje o prawie do wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;
e) informacje o prawie żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych odnoszącego się do osoby, której dane dotyczą.

2. Państwa członkowskie zapewniają, by oprócz informacji, o których mowa w ust. 1, w konkretnych przypadkach administrator przekazywał osobie, której dane dotyczą, następujące dalsze informacje umożliwiające wykonywanie przysługujących jej praw:

a) podstawa prawna przetwarzania;
b) okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
c) w stosownym przypadku kategorie odbiorców danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
d) w razie potrzeby dalsze informacje, zwłaszcza gdy dane osobowe są zbierane bez wiedzy osoby, której dotyczą.

3. Państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, przewidziane w ust. 2 w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
b) uniemożliwić zakłócanie zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar;
c) chronić bezpieczeństwo publiczne;
d) chronić bezpieczeństwo narodowe;
e) chronić prawa i wolności innych osób.

4. Państwa członkowskie mogą przyjąć akty prawne dla określenia kategorii przetwarzania, które w całości lub części wchodzą w zakres stosowania środków wskazanych w którejkolwiek z liter ust. 3.

Artykuł 14. Prawo dostępu przysługujące osobie, której dane dotyczą

Z zastrzeżeniem art. 15 państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli takie dane są przetwarzane, prawo dostępu do danych osobowych i do następujących informacji:

a) cele i podstawa prawna przetwarzania;
b) kategorie odnośnych danych osobowych;
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
d) w miarę możliwości planowany okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
e) informacje o prawie do żądania od administratora sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby;
f) informacje o prawie wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;
g) wskazanie, jakie dane osobowe są przetwarzane, oraz wszelkie dostępne informacje o ich pochodzeniu.

Artykuł 15. Ograniczenia prawa dostępu

1. Państwa członkowskie mogą przyjąć akty prawne pozwalające ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;
c) chronić bezpieczeństwo publiczne;
d) chronić bezpieczeństwo narodowe;
e) chronić prawa i wolności innych osób.

2. Państwa członkowskie mogą przyjąć akty prawne, aby ustalić kategorie przetwarzania, które w całości lub części wchodzą w zakres stosowania ust. 1 lit. a)–e).

3. W przypadkach, o których mowa w ust. 1 i 2, państwa członkowskie zapewniają, by administrator bez zbędnej zwłoki informował pisemnie osobę, której dane dotyczą, o każdej odmowie lub o każdym ograniczeniu dostępu i o przyczynach tej odmowy lub tego ograniczenia. Informacje takie można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z celów, o których mowa w ust. 1. Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

4. Państwa członkowskie zapewniają, by administrator dokumentował faktyczne lub prawne powody, na jakich opiera się decyzja. Informacje te udostępnia się organom nadzorczym.

Artykuł 16. Prawo do sprostowania lub usunięcia danych osobowych oraz ograniczenia ich przetwarzania

1. Państwa członkowskie zapewniają, by osoba, której dane dotyczą, miała prawo uzyskania od administratora sprostowania bez zbędnej zwłoki jej danych osobowych, jeżeli są nieprawidłowe. Mając na względzie cel przetwarzania, państwa członkowskie zapewniają, by osoba, której dane dotyczą, miała prawo uzyskania uzupełnienia

niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

2. Państwa członkowskie nakładają na administratora wymóg usunięcia bez zbędnej zwłoki danych osobowych i zapewniają, by osoba, której dane dotyczą, miała prawo uzyskać od administratora usunięcie bez zbędnej zwłoki jej danych osobowych, jeżeli przetwarzanie narusza przepisy przyjęte na podstawie art. 4, 8 i 10, lub jeżeli dane osobowe muszą zostać usunięte w celu wypełnienia obowiązku prawnego ciążącego na administratorze.

3. Zamiast usunięcia, administrator ogranicza przetwarzanie, jeżeli:

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

Jeżeli przetwarzanie jest ograniczone na mocy akapitu pierwszego lit. a), przed zniesieniem tego ograniczenia administrator informuje o tym osobę, której dane dotyczą.

4. Państwa członkowskie zapewniają, by administrator informował pisemnie osobę, której dane dotyczą, o każdej odmowie sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych oraz o przyczynach tej odmowy. Państwa członkowskie mogą przyjąć akty prawne, które w całości lub w części ograniczają obowiązek udzielania takich informacji, jeżeli takie ograniczenie przetwarzania jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar;

c) chronić bezpieczeństwo publiczne;
d) chronić bezpieczeństwo narodowe;
e) chronić prawa i wolności innych osób.

Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

5. Państwa członkowskie zapewniają, by administrator informował o sprostowaniu nieprawidłowych danych osobowych właściwy organ, od którego nieprawidłowe dane pochodzą.

6. Państwa członkowskie zapewniają, by w przypadkach sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania, na podstawie ust. 1, 2 i 3, administrator miał obowiązek powiadomienia o tym odbiorców, a odbiorcy mieli obowiązek sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych.

Artykuł 17. Wykonywanie praw osoby, której dane dotyczą, oraz weryfikacja dokonywana przez organ nadzorczy

1. W odniesieniu do przypadków, o których mowa w art. 13 ust. 3, art. 15 ust. 3 i art. 16 ust. 4, państwa członkowskie przyjmują środki przewidujące, że osoba, której dane dotyczą, może wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego.

2. Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wykonywania przysługujących jej praw za pośrednictwem organu nadzorczego na mocy ust. 1.

3. W razie wykonywania prawa, o którym mowa w ust. 1, organ nadzorczy informuje osobę, której dane dotyczą, przynajmniej o fakcie przeprowadzenia wszelkich niezbędnych weryfikacji lub przegląd-

dów. Organ nadzorczy informuje osobę, której dane dotyczą, także o przysługującym jej prawie do wniesienia środka prawnego do sądu.

Artykuł 18. Prawa osoby, której dane dotyczą, w postępowaniu przygotowawczym i sądowym w sprawie karnej

Państwa członkowskie mogą zapewnić, by wykonywanie praw, o których mowa w art. 13, 14 i 16, odbywało się zgodnie z prawem państwa członkowskiego, jeżeli dane osobowe znajdują się w orzeczeniu sądu, protokole lub aktach sprawy przetwarzanych w toku postępowania przygotowawczego lub sądowego w sprawie karnej.

Rozdział IV Administrator i podmiot przetwarzający

Sekcja 1 Obowiązki ogólne

Artykuł 19. Obowiązki administratora

1. Państwa członkowskie zapewniają, by administrator wdrażał – uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszą dyrektywą i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Artykuł 20. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Państwa członkowskie zapewniają, by – uwzględniając 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 – administrator zarówno w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, miał obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, takich 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 dyrektywy oraz chronić prawa osób, których dane dotyczą.

2. Państwa członkowskie zapewniają, by administrator wdrażał 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 zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji osoby fizycznej nieokreślonej liczbie osób fizycznych.

Artykuł 21. Współadministratorzy.

1. Państwa członkowskie zapewniają, by w przypadku gdy co najmniej dwaj administratorzy wspólnie ustalają cele i sposoby przetwarzania, byli oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają podział swych obowiązków w zakresie wypełnienia niniejszej dyrektywy, w szczególności w odniesieniu do wykonywania przez osobę, któ-

rej dane dotyczą, przysługujących jej praw, oraz podział obowiązków w zakresie udzielania informacji, o których mowa w art. 13, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach wskazuje się punkt kontaktowy dla osób, których dane dotyczą. Państwa członkowskie mogą wskazać, który ze współadministratorów może pełnić funkcję pojedynczego punktu kontaktowego wobec osób, których dane dotyczą, w celu wykonywania ich praw.

2. Niezależnie od uzgodnień, o których mowa w ust. 1, państwa członkowskie mogą ustanowić, że osoba, której dane dotyczą, może wykonywać prawa przysługujące jej na mocy przepisów przyjętych na podstawie niniejszej dyrektywy w odniesieniu do każdego z administratorów i przeciwko każdemu z nich.

Artykuł 22. Podmiot przetwarzający

1. Państwa członkowskie zapewniają, by – jeżeli przetwarzanie ma być dokonywane w imieniu administratora – administrator miał obowiązek korzystania z usług wyłącznie takich podmiotów przetwarzających, które dają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, oraz zapewniał, by przetwarzanie odpowiadało wymogom niniejszej dyrektywy i chroniło prawa osoby, której dane dotyczą.

2. Państwa członkowskie zapewniają, by podmiot przetwarzający nie korzystał z usług innego podmiotu przetwarzającego bez wcześniejszej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

3. Państwa członkowskie zapewniają, by przetwarzanie przez podmiot przetwarzający było regulowane umową lub innym instrumentem prawnym prawa Unii lub prawa państwa członkowskiego, które wiąże podmiot przetwarzający z administratorem oraz określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz prawa i obowiązki administratora. Taka umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) działa wyłącznie zgodnie z poleceniami administratora;
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) wszelkimi odpowiednimi sposobami pomaga administratorowi w przestrzeganiu przepisów o prawach osoby, której dane dotyczą;
d) po zakończeniu świadczenia usługi przetwarzania danych, w zależności od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego wymaga przechowywanie danych osobowych;
e) udostępnia administratorowi wszelkie informacje niezbędne do wykazania zgodności z niniejszym artykułem;
f) przestrzega warunków zaangażowania innego podmiotu przetwarzającego, o których mowa w ust. 2 i 3.

4. Umowa lub inny akt prawny, o których mowa w ust. 3, mają formę pisemną, w tym formę elektroniczną.

5. Jeżeli podmiot przetwarzający określi, z naruszeniem niniejszej dyrektywy, cele i sposoby przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Artykuł 23. Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego

Państwa członkowskie zapewniają, by podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzała je wyłącznie zgodnie z poleceniami administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Artykuł 24. Wykazy czynności przetwarzania

1. Państwa członkowskie zapewniają, by administratorzy prowadzili wykaz wszystkich kategorii czynności przetwarzania, za które odpowiadają. W wykazie tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe administratora i, w razie potrzeby, współadministratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
d) opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych;
e) w stosownym przypadku informacje o stosowaniu profilowania;
f) w stosownym przypadku kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
g) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;
h) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
i) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 29 ust. 1.

2. Państwa członkowskie zapewniają, by podmioty przetwarzające prowadziły wykaz wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, w którym znajdują się:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających, każdego administratora, w imieniu którego działa podmiot przetwarzający, oraz, w razie potrzeby, inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) w stosownym przypadku przypadki przekazania danych osobowych do państw trzecich lub organizacji międzynarodowej, w razie jednoznacznego polecenia administratora, łącznie z nazwą tego państwa trzeciego lub organizacji międzynarodowej;
d) w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 29 ust. 1.

3. Wykazy, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną. Administrator i podmiot przetwarzający udostępniają wskazane wykazy organowi nadzorczemu na jego żądanie.

Artykuł 25. Ewidencja czynności

1. Państwa członkowskie zapewniają, by ewidencjonowano przynajmniej następujące operacje przetwarzania prowadzone w zautomatyzowanych systemach przetwarzania: zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie i usuwanie. Ewidencja przeglądania i ujawniania pozwala ustalić zasadność, datę i godzinę takich operacji oraz w miarę możliwości tożsamość osoby, która przeglądała lub ujawniła dane osobowe, oraz tożsamość odbiorców takich danych osobowych.

2. Ewidencja jest używana wyłącznie do weryfikacji zgodności przetwarzania z prawem, do monitorowania własnej działalności,

zapewnienia integralności i bezpieczeństwa danych osobowych oraz na potrzeby postępowania karnego.

3. Administrator i podmiot przetwarzający na żądanie udostępniają ewidencję organowi nadzorczemu.

Artykuł 26. Współpraca z organem nadzorczym

Państwa członkowskie zapewniają, by administrator i podmiot przetwarzający współpracowali z organem nadzorczym, na jego żądanie, w ramach wykonywania jego zadań.

Artykuł 27. Ocena skutków dla ochrony danych

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

2. Ocena, o której mowa w ust. 1, zawiera co najmniej ogólny opis planowanych operacji przetwarzania, ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą, środki planowane w celu rozwiązania takiego ryzyka, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazanie zgodności z niniejszą dyrektywą, z uwzględnieniem praw i uzasadnionych interesów osób, których dane dotyczą, i innych zainteresowanych osób.

Artykuł 28. Uprzednie konsultacje z organem nadzorczym

1. Państwa członkowskie zapewniają, by administrator lub podmiot przetwarzający przed przetwarzaniem danych osobowych, które

będzie częścią mającego powstać nowego zbioru danych, skonsultowali się z organem nadzorczym, jeżeli:

a) ocena skutków dla ochrony danych, o której mowa w art. 27, wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka; lub
b) odnośny rodzaj przetwarzania – zwłaszcza z użyciem nowych technologii, mechanizmów lub procedur – stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą.

2. Państwa członkowskie zapewniają przeprowadzenie konsultacji z organem nadzorczym w toku przygotowywania projektu aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania.

3. Państwa członkowskie zapewniają, by organ nadzorczy mógł sporządzać wykaz operacji przetwarzania, które wymagają uprzednich konsultacji zgodnie z ust. 1.

4. Państwa członkowskie zapewniają, by administrator przedstawiał organowi nadzorczemu ocenę wpływu na ochronę danych, o której mowa w art. 27, oraz na żądanie wszelkie inne informacje umożliwiające organowi nadzorczemu ocenę zgodności przetwarzania z przepisami, a w szczególności ocenę ryzyka w sferze ochrony danych osobowych osoby, której dane dotyczą, oraz powiązanych zabezpieczeń.

5. Państwa członkowskie zapewniają, by – jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1 niniejszego artykułu, stanowiłoby naruszenie przepisów przyjętych na podstawie niniejszej dyrektywy, w szczególności jeżeli administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy, w terminie do sześciu tygodni po otrzymaniu wniosku o konsultacje, przedstawił administratorowi, a w stosownym przypadku podmiotowi przetwarzającemu, pisemne zalecenia

i mógł skorzystać z uprawnień, o których mowa w art. 47. Termin ten można przedłużyć o kolejny miesiąc ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje administratora oraz, w stosownym przypadku, podmiot przetwarzający o takim przedłużeniu w terminie jednego miesiąca od otrzymania wniosku w sprawie konsultacji, z podaniem przyczyn tego opóźnienia.

Sekcja 2 Bezpieczeństwo danych osobowych

Artykuł 29. Bezpieczeństwo przetwarzania

1. Państwa członkowskie zapewniają, by – uwzględniając stan wiedzy technicznej i koszt wdrożenia i charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – administrator i podmiot przetwarzający mieli obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych dla zagwarantowania poziomu bezpieczeństwa odpowiadającego zagrożeniu, zwłaszcza jeżeli chodzi o przetwarzanie szczególnych kategorii danych osobowych, o których mowa w art. 10.

2. W odniesieniu do zautomatyzowanego przetwarzania każde państwo członkowskie zapewnia, by po ocenie ryzyka administrator lub podmiot przetwarzający wdrożyli środki, które:

a) uniemożliwią osobom nieuprawnionym dostęp do sprzętu używanego do przetwarzania (kontrola dostępu do sprzętu);
b) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
c) zapobiegną nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

d) zapobiegną korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);
e) zapewniają, że osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);
f) pozwolą zweryfikować i ustalić podmioty, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);
g) pozwolą następczo zweryfikować i stwierdzić, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (kontrola wprowadzania danych);
h) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);
i) zapewniają, że w razie awarii można będzie przywrócić zainstalowane systemy (odzyskiwanie);
j) zapewniają działanie funkcji systemu, zgłaszanie występujących w nich błędów (niezawodność) oraz odporność przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

Artykuł 30. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Państwa członkowskie zapewniają, by w przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, w miarę możliwości nie później niż 72 godzin po stwierdzeniu naruszenia, zgłosił naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to stwarzało ryzyko naruszenia praw i wolności osób fizycznych. W przypadku gdy zgłoszenie naruszenia

organowi nadzorczemu nie następuje w terminie 72 godzin, towarzyszy mu uzasadnienie opóźnienia.

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

3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wykazów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu naprawy naruszenia ochrony danych osobowych, w tym w stosownym przypadku zminimalizowania jego ewentualnych negatywnych skutków.

4. Jeżeli – i w takim zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

5. Państwa członkowskie zapewniają, by administrator dokumentował wszelkie naruszenia ochrony danych osobowych, o których mowa w ust. 1, wraz z okolicznościami naruszenia danych osobowych, jego skutkami oraz podjętymi działaniami naprawczymi. Dokumentacja ta pozwala organowi nadzorczemu na weryfikację przestrzegania niniejszego artykułu.

6. Państwa członkowskie zapewniają, by w przypadku gdy naruszenie ochrony danych osobowych dotyczy danych osobowych przesłanych przez lub do administratora innego państwa członkowskiego, informacje, o których mowa w ust. 3, zostały dostarczone bez zbędnej zwłoki administratorowi tego państwa członkowskiego.

Artykuł 31. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Państwa członkowskie zapewniają, by w przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadomił osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

2. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu, opisuje jasnym i prostym językiem charakter naruszenia ochrony danych osobowych i zawiera co najmniej informacje i środki, o których mowa w art. 30 ust. 3 lit. b), c) i d).

3. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu nie jest wymagane, jeżeli spełniony został którykolwiek z następujących warunków:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, zwłaszcza środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wskazanych w ust. 1; lub
c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może zażądać wystosowania przez

administratora zawiadomienia, lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

5. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu można opóźnić, ograniczyć lub pominąć, z zastrzeżeniem warunków i z powodów wskazanych w art. 13 ust. 3.

Sekcja 3 Inspektor ochrony danych

Artykuł 32. Wyznaczenie inspektora ochrony danych

1. Państwa członkowskie zapewniają, by administrator wyznaczył inspektora ochrony danych. Państwa członkowskie mogą zwolnić z tego obowiązku sądy i inne niezawisłe organy sądowe w ramach sprawowania przez te organy wymiaru sprawiedliwości.

2. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 34.

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

4. Państwa członkowskie zapewniają, by administrator opublikował dane kontaktowe inspektora ochrony danych i zawiadomił o nich organ nadzorczy.

Artykuł 33. Status inspektora ochrony danych

1. Państwa członkowskie zapewniają, by administrator gwarantował odpowiednie i niezwłoczne włączenie inspektora ochrony danych we wszystkie sprawach dotyczących ochrony danych osobowych.

2. Administrator wspiera inspektora ochrony danych w wypełnianiu zadań, o których mowa w art. 34, zapewniając zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania oraz zasoby niezbędne do podtrzymania jego wiedzy fachowej.

Artykuł 34. Zadania inspektora ochrony danych

Państwa członkowskie zapewniają, by administrator powierzył inspektorowi ochrony danych co najmniej następujące zadania:

a) informowanie administratora oraz pracowników zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej dyrektywy oraz na mocy innych przepisów prawa Unii lub państwa członkowskiego dotyczących ochrony danych;
b) monitorowanie przestrzegania niniejszej dyrektywy, innych przepisów prawa Unii lub państwa członkowskiego dotyczących ochrony danych oraz realizowanie polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział obowiązków, działania podnoszące świadomość i szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) przedstawianie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania na mocy art. 27;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego wobec organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 28, oraz w stosownym przypadku prowadzenie konsultacji we wszelkich innych sprawach.

Rozdział V. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Artykuł 35. Ogólne zasady przekazywania danych osobowych

1. Państwa członkowskie zapewniają, by przekazanie przez właściwe organy danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, w tym dalsze przekazane do innego państwa trzeciego lub innej organizacji międzynarodowej, mogło nastąpić pod warunkiem zgodności z przepisami krajowymi przyjętymi na podstawie innych przepisów niniejszej dyrektywy, jedynie jeżeli spełnione zostały warunki ustanowione w niniejszym rozdziale, a mianowicie:

a) przekazanie jest niezbędne do celów, o których mowa w art. 1 ust. 1;
b) dane osobowe są przekazywane administratorowi w państwie trzecim lub organizacji międzynarodowej, który jest organem właściwym do realizacji celów, o których mowa w art. 1 ust. 1;
c) w przypadku przesyłania lub udostępniana danych od innego państwa członkowskiego to inne państwo członkowskie wyraziło na przekazanie uprzednią zgodę zgodnie ze swoim prawem krajowym;
d) Komisja wydała decyzję w przedmiocie zgodności na podstawie art. 36, lub w razie braku takiej decyzji zapewnione zostały lub istnieją odpowiednie zabezpieczenia zgodnie z art. 37, lub w razie braku decyzji w przedmiocie zgodności wydanej na podstawie art. 36 lub zabezpieczeń zgodnie z art. 37, zastosowanie mają wyjątki w szczególnych sytuacjach zgodnie z art. 38; oraz
e) w przypadku dalszego przekazania do innego państwa trzeciego lub organizacji międzynarodowej właściwy organ, który dokonał pierwotnego przekazania, lub inny właściwy organ tego samego państwa członkowskiego zezwala na dalsze przekazanie po należytym uwzględnieniu wszystkich istotnych czynników,

w tym powagi czynu zabronionego, celu, w którym dane osobowe zostały pierwotnie przekazane, oraz stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których dane osobowe są dalej przekazywane.

2. Państwa członkowskie zapewniają, by przekazanie danych osobowych bez uprzedniej zgody innego państwa członkowskiego, o której mowa w ust. 1 lit. c), było dozwolone wyłącznie wtedy, gdy odnośne przekazanie jest niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego w państwie członkowskim lub państwie trzecim bądź dla ważnych interesów państwa członkowskiego, a uprzedniej zgody nie da się uzyskać w odpowiednim terminie. Organ odpowiadający za wydanie uprzedniej zgody zostaje powiadomiony bez zbędnej zwłoki.

3. Wszystkie przepisy niniejszego rozdziału stosuje się w celu zapewnienia, by stopień ochrony osób fizycznych zapewniony niniejszą dyrektywą nie został obniżony.

Artykuł 36. Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony

1. Państwa członkowskie zapewniają, by przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogło nastąpić wtedy, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim, lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

2. Oceniając, czy stopień ochrony jest odpowiedni, Komisja uwzględnia w szczególności następujące elementy:

a) praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie prawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz

dostępu organów publicznych do danych osobowych, a także wdrażanie takiego prawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie trzecim lub w organizacji międzynarodowej, orzecznictwo, a także skuteczne i wykonalne prawa osób, których dane dotyczą, oraz prawa osób, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia;

b) istnienie i skuteczne funkcjonowanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub organu nadzorującego organizację międzynarodową, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym posiadające odpowiednie uprawnienia do egzekwowania przestrzegania przepisów – pomagać i doradzać osobom, których dane dotyczą, w toku wykonywania przysługujących im praw, a także współpracować z organami nadzorczymi państw członkowskich; oraz

c) międzynarodowe zobowiązania państwa trzeciego lub organizacji międzynarodowej lub inne obowiązki wynikające z prawnie wiążących konwencji lub aktów prawnych oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych.

3. Po dokonaniu oceny, czy stopień ochrony jest odpowiedni, w drodze aktu wykonawczego Komisja może zdecydować, że państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu. W akcie wykonawczym przewiduje się mechanizm okresowego przeglądu – przynajmniej raz na cztery lata – podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej. W akcie wykonawczym zostaje

określony terytorialny i sektorowy zakres jego zastosowania, a w stosownym przypadku wskazany zostaje organ nadzorczy lub organy nadzorcze, o których mowa w ust. 2 lit. b) niniejszego artykułu. Akt wykonawczy zostaje przyjęty zgodnie z procedurą sprawdzającą, o której mowa w art. 58 ust. 2.

4. Komisja na bieżąco monitoruje zmiany w państwach trzecich i organizacjach międzynarodowych mogące wpłynąć na obowiązywanie decyzji przyjętych na mocy ust. 3.

5. Jeżeli dostępne informacje tak wskazują, zwłaszcza po przeglądzie, o którym mowa w ust. 3 niniejszego artykułu, Komisja przyjmuje decyzję stwierdzającą, że państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu, i w niezbędnym zakresie uchyla, zmienia lub zawiesza decyzję, o której mowa w ust. 3 niniejszego artykułu, w drodze aktów wykonawczych bez mocy wstecznej. Takie akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 58 ust. 2, lub w przypadkach wyjątkowo pilnych zgodnie z procedurą, o której mowa w art. 58 ust. 2.

W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja przyjmuje zgodnie z procedurą, o której mowa w art. 58 ust. 3, akty wykonawcze mające natychmiastowe zastosowanie.

6. Komisja podejmuje konsultacje z państwem trzecim lub organizacją międzynarodową w celu naprawy sytuacji będącej przyczyną decyzji przyjętej na mocy ust. 5.

7. Państwa członkowskie zapewniają, by decyzja wydana na mocy ust. 5 nie wpływała na przekazywanie danych osobowych do danego państwa trzeciego, terytorium lub jednego lub więcej określonych sektorów w tym państwie trzecim, lub do danej organizacji międzynarodowej na mocy art. 37 i 38.

8. Komisja publikuje w Dzienniku Urzędowym Unii Europejskiej i na swojej stronie internetowej wykaz tych państw trzecich, tery-

toriów i określonych sektorów w państwie trzecim, oraz organizacji międzynarodowych, co do których przyjęła decyzję stwierdzającą odpowiedni stopień ochrony lub jego brak.

Artykuł 37. Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń

1. W razie braku decyzji na mocy art. 36 ust. 3 państwa członkowskie zapewniają, by dane osobowe mogły być przekazane do państwa trzeciego lub organizacji międzynarodowej, jeżeli:

a) w prawnie wiążącym akcie wprowadzono odpowiednie zabezpieczenia ochrony danych osobowych; lub
b) administrator ocenił wszystkie okoliczności związane z przekazaniem danych osobowych i stwierdził, że istnieją odpowiednie zabezpieczenia ochrony danych osobowych.

2. Administrator informuje organ nadzorczy o kategoriach przekazań, o których mowa w ust. 1 lit. b).

3. Jeżeli przekazanie odbywa się na podstawie ust. 1 lit. b), musi być udokumentowane, a dokumentacja, w tym data i godzina przekazania, informacje o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe, musi zostać udostępniona na żądanie organowi nadzorczemu.

Artykuł 38. Wyjątki w szczególnych sytuacjach

1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony na mocy art. 36 lub braku odpowiednich zabezpieczeń określonych w art. 37 państwa członkowskie zapewniają, by przekazanie lub określona kategoria przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogły nastąpić wyłącznie pod warunkiem że przekazanie jest niezbędne:

a) w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby;

b) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą, jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi;
c) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego;
d) w indywidualnym przypadku do celów, o których mowa w art. 1 ust. 1; lub
e) w indywidualnym przypadku, dla ustalenia, dochodzenia lub obrony roszczeń w związku z celami określonymi w art. 1 ust. 1.

2. Danych osobowych nie przekazuje się, jeżeli właściwy organ przekazujący stwierdzi, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem, o którym mowa w ust. 1 lit. d) i e).

3. Jeżeli przekazanie odbywa się na podstawie ust. 1, musi być udokumentowane, a dokumentacja, w tym data i godzina przekazania, informacje o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe, musi zostać udostępniona na żądanie organowi nadzorczemu.

Artykuł 39. Przekazywanie danych osobowych odbiorcom mającym siedzibę w państwach trzecich

1. Na zasadzie wyjątku od art. 35 ust. 1 lit. b) i z zastrzeżeniem umów międzynarodowych, o których mowa w ust. 2 niniejszego artykułu, prawo Unii lub prawo państwa członkowskiego mogą zapewniać, by właściwe organy, o których mowa w art. 3 pkt 7 lit. a), w indywidualnych, konkretnych przypadkach przekazywały dane osobowe bezpośrednio odbiorcom mającym siedzibę w państwach trzecich jedynie wówczas, gdy zachowane są pozostałe przepisy niniejszej dyrektywy i spełnione zostały wszystkie następujące warunki:

a) przekazanie jest ściśle niezbędne do wykonania zadania właściwego organu przekazującego zgodnie z prawem Unii lub prawem państwa członkowskiego do celów, o których mowa w art. 1 ust. 1;
b) właściwy organ przekazujący stwierdza, że podstawowe prawa i wolności danej osoby, której dane dotyczą, nie są nadrzędne wobec interesu publicznego przemawiającego za przedmiotowym przekazaniem;
c) właściwy organ przekazujący uznaje, że przekazanie organowi właściwemu do celów, o których mowa w art. 1 ust. 1, w państwie trzecim byłoby nieskuteczne lub niewłaściwe, w szczególności dlatego, że przekazanie nie może nastąpić w odpowiednim terminie;
d) organ, który jest właściwy dla celów wskazanych w art. 1 ust. 1 w państwie trzecim, zostaje poinformowany bez zbędnej zwłoki, chyba że byłoby to nieskuteczne lub niewłaściwe; oraz
e) właściwy organ przekazujący informuje odbiorcę o konkretnym celu lub konkretnych celach, w których dane osobowe mają być wyłączenie przetwarzane przez odbiorcę, pod warunkiem że takie przetwarzanie jest niezbędne.

2. Umowa międzynarodowa, o której mowa w ust. 1, oznacza jakąkolwiek dwustronną lub wielostronną umowę międzynarodową obowiązującą między państwami członkowskimi a państwami trzecimi dotyczącą współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

3. Właściwy organ przekazujący informuje organ nadzorczy o przekazaniach na mocy niniejszego artykułu.

4. Jeżeli przekazanie odbywa się na podstawie ust. 1, musi być udokumentowane.

Artykuł 40. Międzynarodowa współpraca na rzecz ochrony danych osobowych

Komisja i państwa członkowskie podejmują wobec państw trzecich i organizacji międzynarodowych odpowiednie działania na rzecz:

a) wypracowania mechanizmów współpracy międzynarodowej ułatwiających skuteczne egzekwowanie przepisów o ochronie danych osobowych;
b) zapewnienia wzajemnej pomocy międzynarodowej w egzekwowaniu przepisów o ochronie danych osobowych, w tym poprzez powiadomienia, przekazywanie skarg, pomoc w prowadzeniu postępowań wyjaśniających oraz wymianę informacji, z zastrzeżeniem odpowiednich zabezpieczeń ochrony danych osobowych i innych podstawowych praw i wolności;
c) włączenia stosownych zainteresowanych podmiotów, których sprawa dotyczy, w dyskusję i działalność mające na celu upowszechnianie międzynarodowej współpracy w dziedzinie egzekwowania przepisów o ochronie danych osobowych;
d) upowszechnienia wymiany i dokumentowania przepisów i praktyk w dziedzinie ochrony danych osobowych, w tym dotyczących kolizji jurysdykcyjnych z państwami trzecimi.

Rozdział VI. Niezależne organy nadzorcze

Sekcja 1.Niezależny status.

Artykuł 41. Organ nadzorczy

1. Państwo członkowskie zapewnia, by za monitorowanie stosowania niniejszej dyrektywy odpowiadał co najmniej jeden niezależny organ publiczny, dla ochrony podstawowych praw i wolności osób

fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii (organ nadzorczy).

2. Każdy organ nadzorczy przyczynia się do spójnego stosowania niniejszej dyrektywy w całej Unii. W tym celu organy nadzorcze współpracują ze sobą i z Komisją zgodnie z rozdziałem VII.

3. Państwa członkowskie mogą zapewnić, by organem nadzorczym, o którym mowa w niniejszej dyrektywie i na którym spoczywa obowiązek realizacji zadań organu nadzorczego mającego powstać na mocy ust. 1, mógł zostać organ nadzorczy ustanowiony na mocy rozporządzenia (UE) 2016/679.

4. Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, państwo to wyznacza organ nadzorczy, który ma reprezentować te organy w Europejskiej Radzie Ochrony Danych, o której mowa w art. 51.

Artykuł 42. Niezależność

1. Państwa członkowskie zapewniają, by każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszą dyrektywą działał w sposób w pełni niezależny.

2. Państwa członkowskie zapewniają, by członek lub członkowie ich organów nadzorczych podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszą dyrektywą pozostawali wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracali się do nikogo o instrukcje ani ich od nikogo nie przyjmowali.

3. Członkowie organów nadzorczych państw członkowskich powstrzymują się od wszelkich czynności sprzecznych ze swoimi obowiązkami i podczas swojej kadencji nie podejmują żadnego zajęcia zarobkowego ani niezarobkowego sprzecznego z tymi obowiązkami.

4. Państwa członkowskie zapewniają, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędną do skutecznego wypeł-

niania swoich zadań i wykonywania swoich uprawnień, w tym w kontekście wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych.

5. Państwa członkowskie zapewniają, by każdy organ nadzorczy wybierał i posiadał własny personel, działający pod wyłącznym kierownictwem członka lub członków danego organu nadzorczego.

6. Państwa członkowskie zapewniają, by ich organy nadzorcze podlegały kontroli finansowej w sposób nienaruszający ich niezależności, oraz by dysponowały odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.

Artykuł 43. Ogólne warunki dotyczące członków organu nadzorczego

1. Państwa członkowskie zapewniają, by każdy członek organu nadzorczego był powołany na drodze przejrzystej procedurze przez
- parlament,
- rząd,
- głowę państwa lub
- niezależny organ uprawniony do powoływania członków organu nadzorczego na podstawie prawa państwa członkowskiego.

2. Każdy członek musi posiadać kwalifikacje, doświadczenie i umiejętności, w szczególności w dziedzinie ochrony danych osobowych, potrzebne do wypełniania swoich obowiązków i wykonywania swoich uprawnień.

3. W razie upływu kadencji, rezygnacji lub przymusowego pozbawienia funkcji członek organu przestaje pełnić swoje obowiązki zgodnie z prawem danego państwa członkowskiego.

4. Członek zostaje odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki potrzebne do wypełniania obowiązków.

Artykuł 44. Zasady ustanawiania organu nadzorczego

1. Każde państwo członkowskie określa w swoich przepisach prawnych wszystkie poniższe kwestie:

a) ustanowienie każdego z organów nadzorczych;
b) kwalifikacje i warunki wyboru wymagane do powołania na stanowisko członka swych organów nadzorczych;
c) zasady i procedury powołania członka lub członków każdego z organów nadzorczych;
d) długość kadencji członka lub członków każdego z organów nadzorczych, nie krótszy niż cztery lata, z wyjątkiem pierwszej kadencji po dniu 6 maja 2016 r., która to kadencja może częściowo trwać krócej, jeżeli jest to niezbędne dla ochrony niezależności organu nadzorczego w drodze procedury stopniowej wymiany członków;
e) możliwość ponownego powołania członka lub członków każdego z organów nadzorczych, oraz liczbę kadencji;
f) zasady regulujące obowiązki członka lub członków oraz personelu każdego z organów nadzorczych, zakaz podejmowania sprzecznych z nimi działań, zajęć i czerpania korzyści, w trakcie kadencji oraz po jej zakończeniu, a także przepisy regulujące ustanie stosunku pracy.

2. Członek lub członkowie oraz personel każdego z organów nadzorczych podlegają zgodnie z prawem Unii lub prawem państwa członkowskiego obowiązkowi dochowania tajemnicy służbowej – w trakcie kadencji oraz po jej zakończeniu – w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wypełniania zadań lub wykonywania swoich uprawnień. Obowiązek dochowania tajemnicy służbowej w trakcie kadencji dotyczy zwłaszcza sytuacji, w których osoby fizyczne zgłaszają naruszenia niniejszej dyrektywy.

Sekcja 2. Właściwość, zadania i uprawnienia

Artykuł 45. Właściwość

1. Państwa członkowskie zapewniają, by każdy organ nadzorczy był właściwy do wypełniania przeznaczonych mu zadań i wykonywania uprawnień powierzonych mu zgodnie z niniejszą dyrektywą na terytorium swego państwa członkowskiego.

2. Państwa członkowskie zapewniają, by żaden organ nadzorczy nie był właściwy do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku sprawowania przez nie wymiaru sprawiedliwości. Państwa członkowskie mogą postanowić, że organ nadzorczy nie jest właściwy do nadzorowania operacji przetwarzania dokonywanych przez inne niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie wymiaru sprawiedliwości.

Artykuł 46. Zadania

1. Państwa członkowskie zapewniają, by na ich terytorium każdy organ nadzorczy:

a) monitorował i egzekwował stosowanie przepisów przyjętych na podstawie niniejszej dyrektywy oraz jej aktów wykonawczych;
b) upowszechniał w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk;
c) doradzał, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie ustawowych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem;
d) upowszechniał wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszej dyrektywy;

e) udzielał osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących jej na mocy niniejszej dyrektywy, a w stosownym przypadku współpracował w tym celu z organami nadzorczymi innych państw członkowskich;
f) rozpatrywał skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenia zgodnie z art. 55, w odpowiednim zakresie prowadził postępowanie w przedmiocie tych skarg i w rozsądnym terminie informował skarżącego o postępach i wynikach takiego postępowania, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowania lub koordynacja działań z innym organem nadzorczym;
g) sprawdzał zgodność przetwarzania z prawem na mocy art. 17 oraz informował osobę, której dane dotyczą, w rozsądnym terminie o wynikach tej kontroli zgodnie z ust. 3 tego artykułu lub o powodach jej nieprzeprowadzenia;
h) współpracował z innymi organami nadzorczymi, w tym dzielił się informacjami oraz świadczył wzajemną pomoc w celu zapewnienia spójnego stosowania i egzekwowania niniejszej dyrektywy;
i) prowadził postępowania w sprawie stosowania niniejszej dyrektywy, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;
j) monitorował zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności rozwój technologii informacyjno-komunikacyjnych;
k) pełnił funkcje konsultacyjne, o których mowa w art. 28, co do operacji przetwarzania; oraz
l) brał udział w pracach Europejskiej Rady Ochrony Danych.

2. Każdy organ nadzorczy ułatwia wnoszenie skarg, o których mowa w ust. 1 lit. f), za pomocą takich środków jak gotowy formularz skargi, który można również wypełnić elektronicznie, co nie wyklucza innych sposobów komunikacji.

3. Każdy organ nadzorczy bezpłatnie wypełnia zadania na rzecz osoby, której dane dotyczą, i inspektora ochrony danych.

4. Jeżeli żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, zwłaszcza ze względu na swą powtarzalność, organ nadzorczy może pobrać rozsądną opłatę wynikającą z kosztów administracyjnych lub może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na organie nadzorczym.

Artykuł 47. Uprawnienia

1. Państwa członkowskie zapewniają, by każdy organ nadzorczy posiadał skuteczne uprawnienia w zakresie prowadzenia postępowań. Uprawnienia te obejmują co najmniej uprawnienie do uzyskania od administratora i podmiotu przetwarzającego dostępu do wszelkich przetwarzanych danych osobowych i wszelkich informacji niezbędnych do wypełnienia jego zadań.

2. Państwa członkowskie zapewniają, by każdy organ nadzorczy posiadał skuteczne uprawnienia naprawcze, przykładowo takie jak:

a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu, zgodnie z którymi planowane operacje przetwarzania mogą skutkować naruszeniem przepisów przyjętych na podstawie niniejszej dyrektywy;
b) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji do przepisów przyjętych na podstawie niniejszej dyrektywy, w razie potrzeby w konkretny sposób i w konkretnym terminie, zwłaszcza poprzez nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania zgodnie z art. 16;
c) wprowadzenie czasowych lub stałych ograniczeń przetwarzania, w tym zakazu przetwarzania.

3. Państwa członkowskie zapewniają, by każdy organ nadzorczy posiadał skuteczne uprawnienia doradcze pozwalające przedstawić administratorowi zalecenia zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 28, oraz by z własnej inicjatywy lub

na wniosek mógł wydawać opinie skierowane do parlamentu narodowego, rządu lub, zgodnie z jego prawem krajowym, innych instytucji i organów oraz do społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych.

4. Wykonywanie uprawnień powierzonych organowi nadzorczemu na mocy niniejszego artykułu podlega odpowiednim gwarancjom, w tym prawu do skutecznego środka prawnego przed sądem i rzetelnego procesu, określonym w prawie Unii i prawie państwa członkowskiego zgodnie z Kartą.

5. Państwa członkowskie zapewniają, by każdy organ nadzorczy miał uprawnienie do wniesienia do organów sądowych sprawy dotyczącej naruszenia przepisów przyjętych na podstawie niniejszej dyrektywy oraz, w stosownym przypadku, do wszczęcia lub udziału w inny sposób w postępowaniu sądowym mającym na celu egzekwowanie przepisów przyjętych na podstawie niniejszej dyrektywy.

Artykuł 48. Zgłaszanie naruszeń

Państwa członkowskie zapewniają, by właściwe organy wprowadziły skuteczne mechanizmy zachęcania do poufnego zgłaszania naruszeń niniejszej dyrektywy.

Artykuł 49. Sprawozdania z działalności

Każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu naruszeń i rodzaje nałożonych kar. Sprawozdania są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem krajowym. Są one udostępniane opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

Rozdział VII. Współpraca

Artykuł 50. Wzajemna pomoc

1. Państwa członkowskie zapewniają, by ich organy nadzorcze przekazywały sobie stosowne informacje i świadczyły sobie wzajemną pomoc w celu spójnego wdrażania i stosowania niniejszej dyrektywy oraz wprowadziły środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o przeprowadzenie konsultacji, kontroli i postępowań.

2. Państwa członkowskie zapewniają, by każdy organ nadzorczy podjął wszelkie odpowiednie środki, by odpowiedzi na wniosek innego organu nadzorczego udzielić bez zbędnej zwłoki, nie później niż w terminie jednego miesiąca po otrzymaniu wniosku. Środki takie mogą obejmować w szczególności przekazanie odpowiednich informacji o przebiegu postępowania.

3. Wnioski o pomoc zawierają wszelkie niezbędne informacje, w tym cel i uzasadnienie wniosku. Uzyskane informacje są wykorzystywane wyłącznie do celu, w którym o nie wystąpiono.

4. Organ nadzorczy, do którego skierowano wniosek o pomoc, nie może odmówić jego wykonania, chyba że:

a) nie jest organem właściwym w zakresie przedmiotu wniosku lub środków, o których wykonanie wystąpiono;
lub

b) wykonanie wniosku naruszyłoby niniejszą dyrektywę lub prawo Unii lub prawo państwa członkowskiego, któremu podlega organ nadzorczy, który otrzymał wniosek.

5. Organ nadzorczy, do którego skierowano wniosek, informuje organ nadzorczy, od którego wniosek pochodzi, o wynikach lub, w razie potrzeby, o postępach lub środkach podjętych w celu udzielenia odpowiedzi na ten wniosek. Organ nadzorczy, do którego skiero-

wano wniosek o pomoc, przedstawia powody odmowy nieuwzględnienia wniosku zgodnie z ust. 4.

6. Informacje, o które zwróciły się inne organy nadzorcze, organ nadzorczy, do którego skierowano wniosek o pomoc, co do zasady przekazuje drogą elektroniczną w standardowym formacie.

7. Organy nadzorcze, do których skierowano wniosek o pomoc, nie pobierają opłaty za działania podejmowane w związku z wnioskiem o wzajemną pomoc. Organy nadzorcze mogą uzgodnić zasady wzajemnej rekompensaty wydatków poniesionych w wyniku świadczenia wzajemnej pomocy w wyjątkowych okolicznościach.

8. Komisja może określić w drodze aktów wykonawczych formułę i procedury wzajemnej pomocy, o których mowa w niniejszym artykule, oraz zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych. Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 58 ust. 2.

Artykuł 51. Zadania Europejskiej Rady Ochrony Danych

1. Europejska Rada Ochrony Danych ustanowiona rozporządzeniem (UE) 2016/679 wypełnia następujące zadania w odniesieniu do przetwarzania wchodzącego w zakres zastosowania niniejszej dyrektywy:

a) doradza Komisji w każdej sprawie związanej z ochroną danych osobowych w Unii, w tym w sprawie wszelkich proponowanych zmian do niniejszej dyrektywy;
b) z własnej inicjatywy, na wniosek jednego ze swoich członków lub na wniosek Komisji bada wszelkie kwestie dotyczące stosowania niniejszej dyrektywy i opracowuje wytyczne, zalecenia i najlepsze praktyki w celu wspierania spójnego stosowania niniejszej dyrektywy;
c) opracowuje wytyczne dla organów nadzorczych w sprawie stosowania środków, o których mowa w art. 47 ust. 1 i 3;

d) opracowuje wytyczne, zalecenia i najlepsze praktyki, o których mowa w lit. b) niniejszego akapitu, określające naruszenia ochrony danych osobowych i zbędną zwłokę w rozumieniu art. 30 ust. 1 i 2 oraz poszczególne okoliczności, w jakich administrator lub podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych;
e) opracowuje wytyczne, zalecenia i najlepsze praktyki zgodnie z lit. b) niniejszego akapitu, określające okoliczności, w jakich naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, o których mowa w art. 31 ust. 1;
f) dokonuje przeglądu praktycznego stosowania wytycznych, zaleceń i najlepszych praktyk, o których mowa w lit. b) i c);
g) przedstawia Komisji opinię na potrzeby oceny, czy stopień ochrony w państwie trzecim, na terytorium lub w jednym lub więcej określonym sektorze państwa trzeciego lub w organizacji międzynarodowej jest odpowiedni, w tym na potrzeby oceny, czy takie państwo trzecie, terytorium, określony sektor lub organizacja międzynarodowa nie przestały zapewniać odpowiedniego stopnia ochrony.
h) wspiera współpracę oraz skuteczną dwustronną i wielostronną wymianę informacji i najlepszych praktyk między organami nadzorczymi;
i) wspiera wspólne programy szkoleń oraz ułatwia wymianę personelu między organami nadzorczymi, a w stosownym przypadku z organami nadzorczymi państw trzecich lub organizacji międzynarodowych;
j) wspiera wymianę wiedzy i dokumentów na temat prawa i praktyki w dziedzinie ochrony danych z organami nadzorczymi odpowiedzialnymi za ochronę danych na świecie.

W odniesieniu do akapitu pierwszego lit. g) Komisja udostępnia Europejskiej Radzie Ochrony Danych wszelką niezbędną dokumentację, w tym korespondencję z rządem państwa trzeciego, terytorium

lub określonym sektorem w tym państwie trzecim lub organizacją międzynarodową.

2. Jeżeli Komisja zwraca się do Europejskiej Rady Ochrony Danych z wnioskiem o opinię, może wskazać termin udzielenia odpowiedzi uwzględniając pilność sprawy.

3. Europejska Rada Ochrony Danych przekazuje swoje opinie, wytyczne, zalecenia i najlepsze praktyki Komisji i komitetowi, o którym mowa w art. 58 ust. 1, oraz podaje je do wiadomości publicznej.

4. Komisja informuje Europejską Radę Ochrony Danych o swoich działaniach w odniesieniu do opinii, wytycznych, zaleceń i najlepszych praktyk opracowanych przez Europejską Radę Ochrony Danych.

Rozdział VIII. Środki ochrony prawnej, odpowiedzialność prawna i sankcje

Artykuł 52. Prawo do wniesienia skargi do organu nadzorczego

1. Z zastrzeżeniem innych środków administracyjnych lub środków prawnych przed sądem, państwa członkowskie zapewniają, by każda osoba, której dane dotyczą, miała prawo wnieść skargę do jednego organu nadzorczego, jeżeli sądzi, że dotyczące jej przetwarzanie danych osobowych narusza przepisy przyjęte na podstawie niniejszej dyrektywy.

2. Państwa członkowskie zapewniają, by – jeżeli skarga nie zostaje wniesiona do organu nadzorczego właściwego zgodnie z art. 45 ust. 1 – organ nadzorczy, do którego wniesiono skargę, miał obowiązek przekazania jej bez zbędnej zwłoki właściwemu organowi nadzorczemu. O przekazaniu skargi poinformowana zostaje osoba, której dane dotyczą.

3. Państwa członkowskie zapewniają, by organ nadzorczy, do którego wniesiono skargę, udzielił osobie, której dane dotyczą, dalszej pomocy na jej wniosek.

4. Właściwy organ nadzorczy informuje osobę, której dane dotyczą, o postępach i wyniku skargi, w tym o możliwości wniesienia sądowego środka ochrony prawnej na mocy art. 53.

Artykuł 53. Prawo do skutecznego środka prawnego przed sądem od decyzji organu nadzorczego

1. Z zastrzeżeniem innych środków administracyjnych lub pozasądowych środków ochrony prawnej państwa członkowskie stanowią prawem, że każda osoba fizyczna lub prawna ma prawo do skutecznego środka prawnego przed sądem od prawnie wiążącej decyzji organu nadzorczego, która jej dotyczy.

2. Z zastrzeżeniem innych środków administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka prawnego przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 45 ust. 1 nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub wyniku rozpatrzenia skargi wniesionej na mocy art. 52.

3. Państwa członkowskie zapewniają, by postępowanie przeciwko organowi nadzorczemu zostało wszczęte przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

Artykuł 54. Prawo do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu

Z zastrzeżeniem dostępnych środków administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego na mocy art. 52, państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do skutecznego środka prawnego przed sądem, jeżeli osoba ta uważa, iż jej prawa ustanowione w przepisach przyjętych na podstawie niniejszej dyrektywy zostały naruszone w skutek przetwarzania jej danych osobowych w sposób niezgodny z tymi przepisami.

Artykuł 55. Reprezentowanie osób, których dane dotyczą

Państwa członkowskie, zgodnie z prawem procesowym państwa członkowskiego, zapewniają osobie, której dane dotyczą, prawo do umocowania organu, organizacji lub zrzeszenia o charakterze niezarobkowym, które zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych, do wniesienia w jej imieniu skargi oraz do wykonywania w jej imieniu praw, o których mowa w art. 52, 53 i 54.

Artykuł 56. Prawo do odszkodowania

Państwa członkowskie zapewniają każdej osobie, która poniosła szkodę majątkową lub niemajątkową w wyniku operacji przetwarzania niezgodnej z prawem lub w wyniku czynności naruszającej przepisy przyjęte na podstawie niniejszej dyrektywy, prawo otrzymania od administratora lub innego organu właściwego w świetle prawa państwa członkowskiego odszkodowania za poniesioną szkodę.

Artykuł 57. Sankcje

Państwa członkowskie przyjmują przepisy określające sankcje za naruszenie przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

Rozdział IX. Akty wykonawcze

Artykuł 58. Procedura komitetowa

1. Komisję wspomaga komitet ustanowiony na mocy art. 93 rozporządzenia (UE) 2016/679. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu zastosowanie ma art. 5 rozporządzenia (UE) nr 182/2011.

3. W przypadku odesłania do niniejszego ustępu zastosowanie ma art. 8 rozporządzenia (UE) nr 182/2011 w związku z jego art. 5.

Rozdział X. Przepisy końcowe

Artykuł 59. Uchylenie decyzji ramowej 2008/977/WSiSW

1. Uchyla się decyzję ramową Rady 2008/977/WSiSW ze skutkiem od dnia 6 maja 2018 r.

2. Odesłania do uchylonej decyzji, o której mowa w ust. 1, należy interpretować jako odesłania do niniejszej dyrektywy.

Artykuł 60. Uprzednio przyjęte akty prawne Unii

Dyrektywa nie wpływa na szczegółowe przepisy o ochronie danych osobowych w aktach prawnych Unii, które weszły w życie do dnia 6 maja 2016 r. w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, które regulują przetwarzanie między państwami członkowskimi oraz dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów w ramach zakresu zastosowania niniejszej dyrektywy.

Artykuł 61. Stosunek do uprzednio zawartych umów międzynarodowych o współpracy wymiarów sprawiedliwości w sprawach karnych oraz o współpracy policyjnej

Umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed dniem 6 maja 2016 r. i które są zgodne z prawem Unii mającym zastosowanie przed tą datą, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

Artykuł 62. Sprawozdanie Komisji

1. Do dnia 6 maja 2022 r., a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszej dyrektywy. Sprawozdania te są publikowane.

2. W ramach tych ocen i przeglądów, o których mowa w ust. 1, Komisja analizuje w szczególności stosowanie i funkcjonowanie rozdziału V w sprawie przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, ze szczególnym uwzględnieniem decyzji przyjętych na mocy art. 36 ust. 3 i art. 39.

3. Na potrzeby ust. 1 i 2, Komisja może wystąpić do państw członkowskich i organów nadzorczych o udzielenie informacji.

4. Dokonując ocen i przeglądów, o których mowa w ust. 1 i 2, Komisja uwzględnia stanowiska i ustalenia Parlamentu Europejskiego, Rady oraz do innych właściwych podmiotów lub źródeł.

5. Komisja może przedkładać, w razie konieczności, odpowiednie wnioski w celu zmiany niniejszej dyrektywy, w szczególności z uwzględnieniem rozwoju wiedzy informatycznej oraz rozwoju społeczeństwa informacyjnego.

6. Do dnia 6 maja 2019 r. Komisja dokonuje przeglądu innych przyjętych przez Unię aktów regulujących przetwarzanie przez właściwe organy do celów określonych w art. 1 ust. 1, w tym aktów, o których mowa w art. 60, w celu oceny konieczności dostosowania ich do niniejszej dyrektywy, i w razie potrzeby przedstawia niezbędne propozycje zmiany takich aktów dla zapewnienia spójnego podejścia do ochrony danych osobowych wchodzących w zakres zastosowania niniejszej dyrektywy.

Artykuł 63. Transpozycja

1. Państwa członkowskie przyjmują i publikują do dnia 6 maja 2018 r. przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Tekst tych przepisów niezwłocznie przekazują Komisji. Państwa członkowskie stosują te przepisy od dnia 6 maja 2018 r.

Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

2. W drodze wyjątku od ust. 1 państwo członkowskie może postanowić, że wyjątkowo, jeżeli wymaga to niewspółmiernie dużego wysiłku, zautomatyzowane systemy przetwarzania utworzone przed

dniem 6 maja 2016 r. zostają dostosowane do art. 25 ust. 1 do dnia 6 maja 2023 r.

3. W drodze wyjątku od ust. 1 i 2 niniejszego artykułu, w wyjątkowych okolicznościach państwo członkowskie może dostosować do art. 25 ust. 1 dany zautomatyzowany system przetwarzania, o którym mowa w ust. 2 niniejszego artykułu, w konkretnym terminie dłuższym niż termin, o którym mowa w ust. 2 niniejszego artykułu, jeżeli inaczej nastąpiłyby poważne problemy w funkcjonowaniu tego systemu. Dane państwo członkowskie informuje Komisję o przyczynach tych poważnych problemów i uzasadnia konkretny termin, w którym ma dostosować dany zautomatyzowany system przetwarzania do art. 25 ust. 1. Ten konkretny termin w żadnym wypadku nie upływa później niż dnia 6 maja 2026 r.

4. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 64. Wejście w życie

Niniejsza dyrektywa wchodzi w życie pierwszego dnia po opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

Artykuł 65. Adresaci

Niniejsza dyrektywa jest skierowana do państw członkowskich.

Sporządzono w Brukseli dnia 27 kwietnia 2016 r.

W imieniu Parlamentu Europejskiego	W imieniu Rady
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Przewodniczący	Przewodniczący

Preambuła (motywy 1–107)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,
uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 ust. 2,
uwzględniając wniosek Komisji Europejskiej,
po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,
uwzględniając opinię Komitetu Regionów[1],
stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[2],
a także mając na uwadze, co następuje:

(1) Ochrona osób fizycznych w zakresie przetwarzania danych osobowych jest jednym z praw podstawowych. Artykuł 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej ”Kartą”) oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

(2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych powinny – niezależnie od ich obywatelstwa czy miejsca zamieszkania – przestrzegać ich podstawowych praw i wolności, zwłaszcza prawa do ochrony danych osobowych. Niniejsza dyrektywa ma przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

[1] Dz.U. C 391 z 18.12.2012, s. 127.
[2] Stanowisko Parlamentu Europejskiego z dnia 12 marca 2014 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz stanowisko Rady w pierwszym czytaniu z dnia 8 kwietnia 2016 r. (dotychczas nieopublikowane w Dzienniku Urzędowym). Stanowisko Parlamentu Europejskiego z dnia 14 kwietnia 2016 r.

(3) Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacznie wzrosła. Technologia pozwala na przetwarzanie danych osobowych na niespotykaną dotąd skalę w celu prowadzenia takich czynności jak zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych lub wykonywanie kar.

(4) Należy ułatwić swobodny przepływ danych osobowych między właściwymi organami do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom na terytorium Unii oraz przekazywania takich danych osobowych do państw trzecich i organizacji międzynarodowych, zapewniając przy tym wysoki stopień ochrony danych osobowych. Przemiany te wymagają stworzenia stabilnych i spójniejszych ram dla ochrony danych osobowych w Unii oraz zdecydowanego egzekwowania ich przepisów.

(5) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady[3] ma zastosowanie do całości przetwarzania danych osobowych w państwach członkowskich, zarówno w sektorze publicznym, jak i prywatnym. Nie ma ona jednak zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty", takiej jak działania w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(6) Decyzja ramowa Rady 2008/977/WSiSW[4] ma zastosowanie do współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Jednak zakres zastosowania tej decyzji ramowej jest ograni-

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

[4] Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350 z 30.12.2008, s. 60).

czony do przetwarzania danych osobowych przesyłanych lub udostępnianych pomiędzy państwami członkowskimi.

(7) Zapewnienie spójnego, wysokiego stopnia ochrony danych osobowych osób fizycznych oraz ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich ma zasadnicze znaczenie dla zapewnienia skutecznej współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. W tym celu należy we wszystkich państwach członkowskich zapewnić równorzędny stopień ochrony praw i wolności 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 tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić prawa osób, których dane dotyczą, oraz obowiązki podmiotów, które przetwarzają dane osobowe, jak i odpowiadające im uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych w państwach członkowskich.

(8) Artykuł 16 ust. 2 TFUE powierza Parlamentowi Europejskiemu i Radzie określenie zasad ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz zasad swobodnego przepływu takich danych.

(9) Na tej podstawie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679[5] ustanawia ogólne przepisy mające chronić osoby fizyczne w związku z przetwarzaniem danych osobowych oraz zapewnić swobodny przepływ danych osobowych w Unii.

(10) W deklaracji nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach kar-

[5] Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych) (zob. s. 1 niniejszego Dziennika Urzędowego).

nych i współpracy policyjnej – załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony – konferencja uznała, że ze względu na szczególny charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej konieczne może okazać się przyjęcie – na podstawie art. 16 TFUE – szczególnych przepisów o ochronie danych osobowych i swobodnym przepływie danych osobowych w tych dziedzinach.

(11) Należy zatem odnieść się do tych dziedzin w odrębnej dyrektywie, która stanowi szczególne przepisy o ochronie 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 tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, z zachowaniem szczególnego charakteru takich czynności. Do takich właściwych organów mogą należeć nie tylko organy publiczne – takie jak organy sądowe, policja lub inne organy ścigania – ale też wszelkie inne organy lub podmioty, którym prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów niniejszej dyrektywy. Jeżeli taki organ lub podmiot przetwarza dane osobowe do celów innych niż cele niniejszej dyrektywy, zastosowanie ma rozporządzenie (UE) 2016/679. Rozporządzenie (UE) 2016/679 ma zatem zastosowanie wtedy, gdy organ lub podmiot zbiera dane osobowe do innych celów, a następnie dalej te dane przetwarza w celu realizacji obowiązku prawnego, któremu podlega. Przykładowo do celów postępowania przygotowawczego, wykrywania lub ścigania czynów zabronionych określone instytucje finansowe zatrzymują przetwarzane przez siebie dane osobowe i udostępniają takie dane osobowe tylko właściwym organom krajowym w konkretnych sytuacjach i w zgodzie z prawem państwa członkowskiego. Organ lub podmiot, który w imieniu takich organów przetwarza dane osobowe w ramach niniejszej dyrektywy, powinien podlegać umowie lub innemu aktowi prawnemu oraz przepisom mającym zgodnie z niniejszą dyrektywą zastosowanie do podmiotu przetwarzającego, podczas gdy

w odniesieniu do przetwarzania danych osobowych przez podmiot przetwarzający spoza zakresu niniejszej dyrektywy zastosowanie rozporządzenia (UE) 2016/679 pozostaje niezmienione.

(12) Czynności policji lub innych organów ścigania koncentrują się na zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, wraz z czynnościami policji podejmowanymi, gdy nie wiadomo, czy dane zdarzenie jest czynem zabronionym. Czynności te mogą też polegać na sprawowaniu władzy poprzez stosowanie środków przymusu takich jak czynności policji podczas demonstracji, dużych imprez sportowych czy zamieszek. Czynności te obejmują również utrzymywanie prawa i porządku jako zadanie powierzone policji lub innym organom ścigania, gdy jest to konieczne do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i dla prawnie chronionych podstawowych interesów społecznych i do zapobiegania takim zagrożeniom, które mogą prowadzić do popełnienia czynu zabronionego. Państwa członkowskie mogą powierzyć właściwym organom inne zadania, które niekoniecznie służą zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom, tak by przetwarzanie danych osobowych w związku z tymi innymi zadaniami – o ile mieści się w zakresie prawa Unii – wchodziło w zakres rozporządzenia (UE) 2016/679.

(13) Czyn zabroniony w rozumieniu niniejszej dyrektywy powinien być autonomicznym pojęciem prawa unijnego, zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości").

(14) Niniejsza dyrektywa nie powinna mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym, ani przetwarzania danych osobowych przez państwa członkowskie podczas czynności, które wchodzą w zakres zastosowania tytu-

łu V rozdział 2 Traktatu o Unii Europejskiej (TUE), nie należy uznawać za czynności wchodzące w zakres niniejszej dyrektywy.

(15) Aby zapewnić jednakowy stopień ochrony osób fizycznych poprzez prawnie wykonalne prawa obowiązujące w całej Unii oraz aby zapobiec różnicom utrudniającym wymianę danych osobowych między właściwymi organami, niniejsza dyrektywa powinna przewidywać zharmonizowane zasady ochrony i swobodnego przepływu danych osobowych przetwarzanych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zbliżenie przepisów państw członkowskich nie powinno skutkować osłabieniem gwarantowanej przez nie ochrony danych osobowych, a wręcz przeciwnie – powinno służyć zapewnieniu wysokiego stopnia ochrony w całej Unii. Państwa członkowskie powinny także móc ustanawiać gwarancje wyższe od przewidzianych w niniejszej dyrektywie dla ochrony praw i wolności osoby, której dane dotyczą, w związku z przetwarzaniem danych osobowych przez właściwe organy.

(16) Niniejsza dyrektywa nie narusza zasady publicznego dostępu do dokumentów urzędowych. W myśl rozporządzenia (UE) 2016/679 dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych.

(17) Ochrona przyznana niniejszą dyrektywą powinna być stosowana do osób fizycznych, bez względu na obywatelstwo czy miejsce zamieszkania, w związku z przetwarzaniem ich danych osobowych.

(18) W celu zapobieżenia wystąpieniu poważnego ryzyka obchodzenia prawa, ochrona osób fizycznych powinna być technologiczne neutral-

na i nie powinna zależeć od stosowanych technik. Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów, jak i ich strony tytułowe, które nie są uporządkowane według określonych kryteriów, nie powinny wchodzić w zakres stosowania niniejszej dyrektywy.

(19) Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii ma zastosowanie rozporządzenie (WE) nr 45/2001[6] Parlamentu Europejskiego i Rady. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych należy dostosować do zasad i przepisów przyjętych w rozporządzeniu (UE) 2016/679.

(20) Niniejsza dyrektywa nie powinna stanowić dla państw członkowskich przeszkody w określaniu – w krajowym prawie karnym procesowym – operacji i procedur przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości, zwłaszcza danych osobowych ujmowanych w orzeczeniach sądowych lub aktach związanych z postępowaniem karnym.

(21) Zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Aby stwierdzić, czy daną osobę fizyczną można zidentyfikować, należy wziąć pod uwagę wszelkie sposoby, takie jak wyodrębnienie, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby fizycznej, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas

[6] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, mianowicie do informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osoby, której dane osobowe dotyczą, nie można już zidentyfikować.

(22) Organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej, takich jak organy podatkowe, organy celne, jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych, nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonych czynności w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądania ujawnienia danych, z którymi występują takie organy publiczne, powinny zawsze mieć formę pisemną, posiadać uzasadnienie, mieć charakter wyjątkowy i nie powinny dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając dane osobowe, takie organy publiczne powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

(23) Dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby fizycznej i wynikające z analizy próbki biologicznej danej osoby, a w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy wszelkich innych materiałów umożliwiających pozyskanie równoważnych informacji. Biorąc pod uwagę złożoność i wrażliwość informacji genetycznych, istnieje wysokie ryzyko niewłaściwego i ponownego ich wykorzystania do nieuprawnionych celów przez administratora. Dyskryminacja oparta na danych genetycznych powinna być co do zasady zakazana.

(24) Do danych osobowych dotyczących zdrowia należy zaliczyć wszelkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie zdrowia fizycznego lub psychicznego osoby, której dane dotyczą. Do danych tych należą informacje o osobie fizycznej zebrane podczas jej rejestracji na potrzeby usług opieki zdrowotnej lub podczas świadczenia usług opieki zdrowotnej takiej osobie, jak to określa dyrektywa 2011/24/UE Parlamentu Europejskiego i Rady[7]; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z laboratoryjnych lub lekarskich badań części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie inne informacje, przykładowo, o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu szpitalnym lub o stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

(25) Wszystkie państwa członkowskie należą do Międzynarodowej Organizacji Policji Kryminalnej (Interpol). Aby wypełnić swoją misję, Interpol otrzymuje, przechowuje i przekazuje dane osobowe w celu wspierania właściwych organów w zapobieganiu i zwalczaniu przestępczości międzynarodowej. W związku z tym należy wzmocnić współpracę między Unią a Interpolem poprzez promowanie sprawnej wymiany danych osobowych, jednocześnie zapewniając poszanowanie podstawowych praw i wolności w przypadku automatycznego przetwarzania danych osobowych. Gdy dane osobowe są przekazywane przez Unię Interpolowi oraz państwom, które oddelegowały swoich przedstawicieli do Interpolu, zastosowanie powinna mieć niniejsza dyrektywa, w szczególności przepisy o międzynarodowym przekazywaniu danych. Niniejsza dyrektywa nie powinna wpływać na stosowanie przepisów szczegółowych określo-

[7] Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

nych we wspólnym stanowisku Rady 2005/69/WSiSW[8] oraz w decyzji Rady 2007/533/WSiSW[9].

(26) Przetwarzanie danych osobowych musi być zgodne z prawem, rzetelne i przejrzyste względem zainteresowanej osoby fizycznej oraz służyć wyłącznie konkretnym celom określonym prawem. Nie stanowi to dla organów ścigania przeszkody w prowadzeniu czynności takich jak nadzór niejawny lub monitoring wizyjny. Czynności takie można prowadzić do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, jeżeli czynności te są określone prawem i stanowią środek niezbędny i proporcjonalny w społeczeństwie demokratycznym, z należytym uwzględnieniem uzasadnionych interesów danej osoby fizycznej. Zasada rzetelnego przetwarzania obowiązująca w ochronie danych jest pojęciem odrębnym względem prawa do rzetelnego procesu, które jest zdefiniowane w art. 47 Karty i w art. 6 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (zwanej dalej „EKPC"). Osobom fizycznym należy uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem ich danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. Wyraźne, uzasadnione i określone w momencie zbierania danych osobowych powinny być w szczególności konkretne cele ich przetwarzania. Dane osobowe powinny być adekwatne i właściwe w stosunku do celów przetwarzania. Należy w szczególności zapewnić, by zebrane dane osobowe nie były nadmierne i by okres ich przechowywania był nie dłuższy, niż jest to niezbędne do osiągnięcia celu ich przetwarzania. Dane osobowe powinny być przetwarzane tylko wtedy, gdy celu przetwarzania nie można rozsądnie osiągnąć innymi sposobami. Aby zapobiec

[8] Wspólne stanowisko Rady 2005/69/WSiSW z dnia 24 stycznia 2005 r. w sprawie wymiany niektórych danych z Interpolem (Dz.U. L 27 z 29.1.2005, s. 61).

[9] Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 205 z 7.8.2007, s. 63).

przechowywaniu danych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Państwa członkowskie powinny ustanowić odpowiednie zabezpieczenia dla danych osobowych przechowywanych dłużej w celu archiwizacji w interesie publicznym, wykorzystania do celów naukowych, statystycznych lub historycznych.

(27) Zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych wymaga, aby właściwe organy przetwarzały dane osobowe – zebrane w kontekście zapobiegania konkretnym czynom zabronionym, prowadzenia postępowań przygotowawczych w ich sprawie, wykrywania ich lub ścigania – w kontekście szerszym, dla lepszego zrozumienia działalności przestępczej oraz ustalenia powiązań pomiędzy różnymi wykrytymi czynami zabronionymi.

(28) Aby zapewnić bezpieczeństwo w stosunku do przetwarzania i zapobiegać przetwarzaniu z naruszeniem niniejszej dyrektywy, dane osobowe należy przetwarzać tak, by zapewnić odpowiedni stopień bezpieczeństwa i poufności, w tym chronić przed nieuprawnionym dostępem do takich danych i do sprzętu służącego ich przetwarzaniu lub przed nieuprawnionym korzystaniem z takich danych i sprzętu, z uwzględnieniem stanu wiedzy technicznej w odnośnej dziedzinie, technologii i kosztów wdrożenia w stosunku do ryzyka naruszenia i charakteru danych osobowych wymagających ochrony.

(29) Dane osobowe należy zbierać w konkretnych, wyraźnych i prawnie uzasadnionych celach mieszczących się w zakresie zastosowania niniejszej dyrektywy i nie należy ich przetwarzać w celach niezgodnych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych i wykonywaniem kar, w tym z ochroną przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiem takim zagrożeniom. Jeżeli dane osobowe przetwarza ten sam lub inny administrator w celu wchodzącym w zakres stosowania niniejszej dyrektywy, ale innym niż cel, w którym dane zostały zebrane, przetwarzanie takie powinno być dopuszczalne, pod warunkiem,

że przetwarzanie jest dozwolone na mocy mających zastosowanie przepisów prawa oraz jest niezbędne i proporcjonalne do tego innego celu.

(30) Zasadę prawidłowości danych należy stosować z uwzględnieniem charakteru i celu odnośnego przetwarzania. W szczególności w postępowaniu sądowym oświadczenia zawierające dane osobowe opierają się na subiektywnym osądzie osób fizycznych i nie zawsze są weryfikowalne. Dlatego wymóg prawidłowości danych nie powinien odnosić się do prawidłowości oświadczenia, lecz jedynie do faktu, że konkretne oświadczenie zostało złożone.

(31) Nieodłączną cechą przetwarzania danych osobowych w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej jest to, że przetwarzane są dane osobowe dotyczące różnych kategorii osób, których dane dotyczą. W stosownych przypadkach należy zatem w jak największym stopniu wyraźnie rozróżniać dane osobowe różnych kategorii osób, których dane dotyczą, takich jak osoby podejrzane, osoby skazane za czyn zabroniony, ofiary i inne osoby, np. świadkowie, osoby posiadające istotne informacje lub kontakty oraz wspólnicy osób podejrzanych i skazanych przestępców. Nie powinno to uniemożliwiać stosowania – zgodnie z wykładnią przedstawioną odpowiednio w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka – zasady domniemania niewinności zagwarantowanej w Karcie oraz w EKPC.

(32) Właściwe organy powinny zapewnić, by nieprawidłowe, niekompletne lub nieaktualne dane osobowe nie były przesyłane ani udostępniane. Aby zapewnić ochronę osób fizycznych, prawidłowość, kompletność i stopień aktualności danych oraz wiarygodność przesyłanych lub udostępnianych danych osobowych, właściwe organy powinny w miarę możliwości opatrywać wszelkie przesyłane dane osobowe niezbędnymi informacjami.

(33) Jeżeli w niniejszej dyrektywie jest mowa o prawie państwa członkowskiego, podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem

wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Takie prawo państwa członkowskiego, podstawa prawna lub akt prawny powinny jednak być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka. Prawo państwa członkowskiego regulujące przetwarzanie danych osobowych w ramach zakresu zastosowania niniejszej dyrektywy powinno co najmniej określać cele ogólne, dane osobowe mające podlegać przetwarzaniu, cele przetwarzania oraz procedury pozwalające chronić integralność i poufność danych osobowych oraz procedury niszczenia tych danych, a tym samym powinno zapewniać dostateczną ochronę przed ryzykiem nadużyć i arbitralności.

(34) Przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, powinno obejmować każdą operację lub każdy zestaw operacji, które wykonuje się do wspomnianych celów na danych osobowych lub na ich zestawach w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, dopasowywanie lub łączenie, ograniczanie przetwarzania, usuwanie lub niszczenie. W szczególności przepisy niniejszej dyrektywy powinny mieć zastosowanie do przesyłania danych osobowych, które służy celom określonym w niniejszej dyrektywie, odbiorcom niepodlegającym niniejszej dyrektywie. Odbiorca taki powinien oznaczać osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, któremu właściwy organ ujawnia te dane zgodnie z prawem. Jeżeli właściwy organ pierwotnie zebrał dane osobowe do jednego z celów określonych w niniejszej dyrektywie, to do przetwarzania tych danych do celów innych niż określone w niniejszej dyrektywie – jeżeli przetwarzanie to jest dozwolone przez prawo Unii lub prawo państwa członkowskiego – powinno mieć zastosowanie rozporządzenie (UE)

2016/679. W szczególności przepisy rozporządzenia (UE) 2016/679 powinny mieć zastosowanie do przesyłania danych osobowych do celów niewchodzących z zakres stosowania niniejszej dyrektywy. Do przetwarzania danych osobowych przez odbiorcę, który nie jest właściwym organem lub nie występuje w charakterze właściwego organu w rozumieniu niniejszej dyrektywy i któremu właściwy organ ujawnia dane osobowe zgodnie z prawem, zastosowanie powinno mieć rozporządzenie (UE) 2016/679. Przy wdrażaniu niniejszej dyrektywy państwa członkowskie powinny też mieć możliwość dalszego doprecyzowania zastosowania przepisów rozporządzenia (UE) 2016/679, na warunkach w nim określonych.

(35) Aby przetwarzanie danych osobowych w ramach niniejszej dyrektywy było zgodne z prawem, powinno ono być niezbędne do wykonania zadań realizowanych przez właściwy organ w interesie publicznym na podstawie prawa Unii lub prawa państwa członkowskiego do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Działania takie powinny obejmować ochronę żywotnych interesów osoby, której dane dotyczą. Wykonywanie zadań polegających na zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, instytucjonalnie powierzonych na mocy prawa właściwym organom, pozwala tym organom wymagać lub nakazywać, aby osoby fizyczne zastosowały się do stawianych żądań. W takim przypadku zgoda osoby, której dane dotyczą, określona w rozporządzeniu (UE) 2016/679, nie powinna stanowić podstawy prawnej przetwarzania danych osobowych przez właściwe organy. Jeżeli osoba, której dane dotyczą, musi wywiązać się z obowiązku prawnego, nie ma ona faktycznego, swobodnego wyboru, a tym samym nie można uznać, iż jej reakcja jest swobodnym wyrazem jej woli. Nie powinno to stanowić dla państw członkowskich przeszkody w ustanowieniu z mocy prawa, że osoba, której dane dotyczą, może wyrazić zgodę na przetwarzanie jej danych osobowych do celów określonych w niniejszej dyrektywie, takich jak badania DNA w postępo-

waniu przygotowawczym czy monitorowanie miejsca jej pobytu za pomocą aparatury elektronicznej na potrzeby wykonania kary.

(36) Państwa członkowskie powinny zapewnić, aby ilekroć prawo Unii lub prawo państwa członkowskiego mające zastosowanie do właściwego organu przesyłającego stawia w określonych sytuacjach szczególne wymogi co do przetwarzania danych osobowych, takie jak stosowanie kodeksów postępowania, właściwy organ przesyłający informował o takich wymogach i o obowiązku ich przestrzegania odbiorcę danych osobowych. Wymogi takie mogą przykładowo obejmować zakaz przesyłania danych osobowych innym odbiorcom lub wykorzystywania ich do innych celów niż cele, dla których przesłano je odbiorcy, lub udzielenia informacji osobie, której dane dotyczą, w przypadku ograniczenia prawa do informacji bez uprzedniej zgody właściwego organu przesyłającego. Obowiązki takie powinny także dotyczyć przekazywania danych przez właściwy organ przesyłający odbiorcom w państwach trzecich lub organizacjach międzynarodowych. Państwa członkowskie powinny zapewnić, by właściwy organ przesyłający nie stosował względem odbiorców w innych państwach członkowskich ani w organach i jednostkach organizacyjnych ustanowionych na mocy tytułu V rozdział 4 i 5 TFUE wymogów innych niż mające zastosowanie do podobnego przesyłania danych w obrębie państwa członkowskiego właściwego organu.

(37) Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko naruszenia podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszej dyrektywie terminu „pochodzenie rasowe" nie oznacza, że Unia akceptuje teorie sugerujące istnienie osobnych ras ludzkich. Takich danych nie należy przetwarzać, chyba że przetwarzanie podlega odpowiednim, określonym prawem gwarancjom praw i wolności osoby, której dane dotyczą, i jest dozwolone w przypadkach dopuszczonych prawem, a jeżeli nie jest dotąd dopuszczone takim prawem – jest niezbędne do ochrony żywotnych interesów oso-

by, której dane dotyczą, lub innej osoby, albo też dotyczy danych w sposób oczywisty upublicznionych przez samą osobę, której dane dotyczą. Odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, mogą obejmować możliwość zbierania takich danych tylko w połączeniu z innymi danymi dotyczącymi danej osoby fizycznej, możliwość odpowiedniego zabezpieczenia takich danych, ściślejsze uregulowanie dostępu pracowników właściwego organu do danych lub zakaz przesyłania danych. Przetwarzanie takich danych powinno być także dozwolone prawem, gdy osoba, której dane dotyczą, udzieliła wyraźnej zgody na szczególnie dla niej inwazyjne przetwarzanie. Niemniej sama zgoda osoby, której dane dotyczą, nie powinna stanowić podstawy prawnej przetwarzania takich wrażliwych danych osobowych przez właściwe organy.

(38) Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie stosowano względem niej decyzji analizującej jej cechy osobiste, opierającej się wyłącznie na przetwarzaniu automatycznym, która ma niekorzystne skutki prawne dla takiej osoby lub poważnie na nią wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, wraz z konkretną informacją dla osoby, której dane dotyczą, i prawem do uzyskania interwencji ludzkiej, a zwłaszcza prawem do wyrażenia własnego stanowiska, uzyskania wyjaśnienia decyzji wydanej wskutek takiej analizy lub zaskarżenia tej decyzji. Profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, powinno być zakazane na warunkach określonych w art. 21 i 52 Karty.

(39) Aby osoba, której dane dotyczą, mogła wykonywać swoje prawa, wszelkie kierowane do niej informacje powinny być łatwo dostępne, także na stronie internetowej administratora, i zrozumiałe, przy użyciu jasnego i prostego języka. Informacje takie powinny być dostosowane do potrzeb osób wymagających szczególnej opieki, np. dzieci.

(40) Należy wprowadzić ułatwienia pozwalające osobie, której dane dotyczą, na wykonywanie praw wynikających z przepisów przyjętych na podstawie niniejszej dyrektywy, w tym mechanizmy żądania – i w stosownych przypadkach bezpłatnego uzyskiwania – w szczególno-

ści dostępu do danych osobowych i ich sprostowania lub usunięcia oraz ograniczenia ich przetwarzania. Administrator powinien mieć obowiązek odpowiadania na żądania osoby, której dane dotyczą, bez zbędnej zwłoki, chyba że stosuje ograniczenia praw osoby, której dane dotyczą, zgodnie z niniejszą dyrektywą. Ponadto, jeżeli żądania są w sposób oczywisty nieuzasadnione lub nadmierne – tak jak wtedy, gdy osoba, której dane dotyczą, nieracjonalnie i ustawicznie żąda informacji lub gdy nadużywa przysługującego jej prawa do informacji, przykładowo podając fałszywe lub mylne dane przy występowaniu z żądaniem – administrator powinien mieć możliwość pobrania rozsądnej opłaty lub odmowy podjęcia działań w stosunku do tego żądania.

(41) W przypadku gdy administrator żąda dodatkowych informacji, aby potwierdzić tożsamość osoby, której dane dotyczą, informacje te powinny być przetwarzane wyłącznie w tym konkretnym celu i nie powinny być przechowywane dłużej niż to konieczne dla realizacji tego celu.

(42) Osobie, której dane dotyczą, należy udostępnić następujące informacje: tożsamość administratora, prowadzenie operacji przetwarzania, cele przetwarzania oraz prawo do wniesienia skargi, istnienie prawa do zażądania od administratora dostępu do danych, sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania. Można to uczynić na stronie internetowej właściwego organu. Ponadto w konkretnych przypadkach i w celu zapewnienia osobie, której dane dotyczą, możliwości wykonywania jej praw, osoba ta powinna być informowana o podstawie prawnej przetwarzania oraz o okresie przechowywania danych, o ile udzielenie takich informacji jest konieczne z uwzględnieniem konkretnych okolicznościach przetwarzania danych, dla zagwarantowania rzetelnego przetwarzania danych tej osoby.

(43) Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania danych i móc zweryfikować jego zgodność z prawem. Dlatego każda osoba, której dane dotyczą, powinna mieć prawo do poznania i uzyskania informacji na temat celów przetwarzania danych, okresu ich

przetwarzania oraz odbiorców danych, także w państwach trzecich. Jeśli takie informacje obejmują informacje o pochodzeniu danych osobowych, nie powinny one ujawniać tożsamości osób fizycznych, w szczególności poufnych źródeł informacji. Dla realizacji tego prawa wystarczy przekazać osobie, której dane dotyczą, pełne podsumowanie tych danych w zrozumiałej formie, czyli w formie pozwalającej jej poznać te dane, sprawdzić ich prawidłowość oraz zweryfikować zgodność ich przetwarzania z niniejszą dyrektywą, tak by mogła ona wykonywać prawa przysługujące jej na mocy niniejszej dyrektywy. Takie podsumowanie może mieć formę kopii przetwarzanych danych osobowych.

(44) Państwa członkowskie powinny mieć możliwość przyjmowania aktów prawnych pozwalających opóźnić, ograniczyć lub pominąć informowanie osób, których dane dotyczą, lub ograniczyć, w całości lub w części, dostęp tych osób do ich własnych danych osobowych w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej – tak aby uniemożliwić zakłócanie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub czynności procesowych, aby uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne lub narodowe lub aby chronić prawa i wolności innych osób. Administrator powinien dokonywać oceny – badając konkretnie i indywidualnie każdy przypadek – czy prawo dostępu powinno zostać częściowo lub całkowicie ograniczone.

(45) Co do zasady o każdej odmowie lub każdym ograniczeniu dostępu należy powiadomić pisemnie osobę, której dane dotyczą, z podaniem faktycznych lub prawnych podstaw decyzji.

(46) Każde ograniczenie praw osoby, której dane dotyczą, musi być zgodne z Kartą i EKPC, w myśl wykładni zawartej, odpowiednio, w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Czło-

wieka, a zwłaszcza musi odbywać się z poszanowaniem istoty tych praw i wolności.

(47) Każda osoba fizyczna powinna mieć prawo do uzyskania sprostowania dotyczących jej nieprawidłowych danych osobowych, zwłaszcza danych dotyczących faktów, oraz prawo do usunięcia danych, jeżeli przetwarzanie takich danych narusza niniejszą dyrektywę. Niemniej prawo do sprostowania danych nie powinno dotyczyć, na przykład, treści zeznania świadka. Każda osoba fizyczna powinna mieć również prawo do ograniczenia przetwarzania danych osobowych, gdy kwestionuje ona ich prawidłowość, której nie da się potwierdzić, lub gdy dane osobowe muszą zostać zachowane do celów dowodowych. W szczególności należy ograniczyć przetwarzanie danych osobowych zamiast ich usuwania, jeżeli w konkretnym przypadku uzasadnione przesłanki sugerują, że usunięcie mogłoby wpłynąć na uprawnione interesy osoby, której dane dotyczą. W takim przypadku ograniczone dane należy przetwarzać tylko w celu, który zapobiegł ich usunięciu. Metody ograniczonego przetwarzania danych osobowych obejmują między innymi przeniesienie wybranych danych do innego systemu przetwarzania – np. do celów archiwizacyjnych – lub uniemożliwienie użytkownikom dostępu do wybranych danych. W zautomatyzowanych zbiorach danych ograniczenie przetwarzania danych osobowych należy zasadniczo zapewnić środkami technicznymi. Fakt ograniczenia przetwarzania danych osobowych należy zaznaczyć w systemie w sposób jasno wskazujący, że przetwarzanie tych danych jest ograniczone. O takim sprostowaniu lub usunięciu danych osobowych lub ograniczeniu ich przetwarzania należy poinformować odbiorców, którym dane zostały ujawnione, oraz właściwe organy, od których pochodzą nieprawidłowe dane. Administratorzy powinni również powstrzymać się od dalszego rozpowszechniania tych danych.

(48) Jeżeli administrator odmawia osobie, której dane dotyczą, prawa do informacji, dostępu lub sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania, osoba, której dane dotyczą, powinna mieć prawo wystąpienia do krajowego organu nadzorczego o weryfikację zgodności przetwarzania z prawem. O prawie tym należy

poinformować osobę, której dane dotyczą. Jeżeli organ nadzorczy podejmie działanie w imieniu osoby, której dane dotyczą, spoczywa na nim obowiązek poinformowania tej osoby co najmniej o fakcie przeprowadzenia wszelkich niezbędnych przeglądów lub kontroli. Organ nadzorczy powinien także poinformować osobę, której dane dotyczą, o przysługującym jej prawie do środka prawnego przed sądem.

(49) Jeżeli dane osobowe przetwarza się w toku postępowania przygotowawczego i sądowego w sprawie karnej, państwa członkowskie powinny mieć możliwość zapewnienia wykonywania prawa do informacji, dostępu lub poprawienia, usunięcia i ograniczenia przetwarzania zgodnie z krajowymi przepisami o postępowaniu sądowym.

(50) Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszą dyrektywą. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Środki podejmowane przez administratora powinny obejmować opracowanie i wdrożenie szczególnych zabezpieczeń w odniesieniu do postępowania z danymi osobowymi osób fizycznych wymagających szczególnej opieki, takich jak dzieci.

(51) Z przetwarzania danych może wynikać ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, której dane dotyczą, to zaś może prowadzić do uszczerbku fizycznego oraz szkód majątkowych i niemajątkowych, w szczególności: gdy przetwarzanie może skutkować dyskryminacją, kradzieżą lub sfałszowaniem tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych chronionych tajemnicą służbową, niedozwolonym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; gdy osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; gdy przetwarzane

są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych; gdy przetwarzane są dane genetyczne lub biometryczne w celu jednoznacznego zidentyfikowania osoby lub jeżeli przetwarzane są dane dotyczące zdrowia lub dane dotyczące seksualności i orientacji seksualnej lub dane o wyrokach skazujących i czynach zabronionych lub o odnośnych środkach zabezpieczających; gdy oceniane są cechy osobowe, w szczególności poprzez analizowanie i prognozowanie okoliczności dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się, w celu tworzenia lub wykorzystywania profili osobistych; gdy przetwarzane są dane osobowe osób fizycznych wymagających szczególnej opieki, zwłaszcza dzieci; lub gdy przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

(52) Prawdopodobieństwo i wagę ryzyka naruszenia należy określić poprzez uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy operacje przetwarzania danych niosą poważne zagrożenie. Wysokie ryzyko jest szczególnym ryzykiem naruszenia praw i wolności osób, których dane dotyczą.

(53) Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszej dyrektywy. Wdrożenie takich środków nie powinno zależeć wyłącznie od względów gospodarczych. Aby móc wykazać przestrzeganie przepisów niniejszej dyrektywy, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Jeśli administrator przeprowadził ocenę skutków dla ochrony danych zgodnie z niniejszą dyrektywą, jej wyniki powinno uwzględniać się przy opracowywaniu wspomnianych środków i procedur. Środki takie mogą polegać między innymi na stosowaniu pseudonimizacji najszybciej,

jak to możliwe. Stosowanie pseudonimizacji do celów niniejszej dyrektywy może być narzędziem ułatwiającym zwłaszcza swobodny przepływ danych osobowych w obszarze wolności, bezpieczeństwa i sprawiedliwości.

(54) Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania jasnego podziału obowiązków przyjętych w niniejszej dyrektywie, w tym w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora.

(55) Przetwarzanie przez podmiot przetwarzający powinno być regulowane aktem prawnym, w tym umową wiążącą podmiot przetwarzający z administratorem i przewidującą w szczególności, że podmiot przetwarzający powinien działać wyłącznie zgodnie z poleceniami administratora. Podmiot przetwarzający powinien uwzględniać zasadę ochrony danych w fazie projektowania oraz zasadę domyślnej ochrony danych.

(56) Dla zachowania zgodności z niniejszą dyrektywą administrator lub podmiot przetwarzający powinni prowadzić wykazy wszystkich kategorii czynności przetwarzania danych osobowych, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinien mieć obowiązek współpracy z organem nadzorczym i na jego żądanie udostępniać wskazane wykazy w celu monitorowania tych operacji przetwarzania. Administrator lub podmiot przetwarzający dane osobowe w niezautomatyzowanych systemach przetwarzania powinien dysponować skutecznymi metodami, które pozwolą mu wykazać zgodność przetwarzania danych z prawem, monitorować własną działalność i zapewnić integralność i bezpieczeństwo danych, takimi jak ewidencja lub inne formy zapisu.

(57) Należy ewidencjonować przynajmniej operacje dokonywane w zautomatyzowanych systemach przetwarzania, takie jak zbieranie,

modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie lub usuwanie danych. Należy ewidencjonować tożsamość osoby, która przeglądała lub ujawniła dane osobowe, co powinno pozwolić na ustalenie uzasadnienia operacji przetwarzania. Ewidencja powinna być używana wyłącznie do weryfikacji zgodności przetwarzania danych z prawem, do monitorowania własnej działalności, zapewniania integralności i bezpieczeństwa danych oraz do celów postępowania karnego. Monitorowanie własnej działalności powinno także obejmować wewnętrzne postępowanie dyscyplinarne przeprowadzane przez właściwe organy.

(58) Ocena skutków dla ochrony danych powinna być przeprowadzana przez administratora, jeżeli operacje przetwarzania – z racji swego charakteru, zakresu lub celów – mogą stwarzać poważne zagrożenie dla praw i wolności osób, których dane dotyczą, i powinna obejmować w szczególności przewidywane środki, gwarancje i mechanizmy mające na celu zapewnienie ochrony danych osobowych oraz wykazanie zgodności z niniejszą dyrektywą. Oceny skutków powinny dotyczyć stosownych systemów i procesów związanych z czynnościami przetwarzaniem danych osobowych, lecz nie indywidualnych przypadków.

(59) Aby zapewnić skuteczną ochronę praw i wolności osób, których dane dotyczą, administrator lub podmiot przetwarzający powinni w określonych przypadkach konsultować się z organem nadzorczym przed przetwarzaniem.

(60) W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu z naruszeniem niniejszej dyrektywy administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz powinni wdrożyć środki – takie jak szyfrowanie – minimalizujące takie ryzyko. Środki takie powinny zapewnić odpowiedni stopień bezpieczeństwa i poufności, oraz uwzględniać stan wiedzy technicznej, koszty ich wdrożenia w stosunku do ryzyka naruszenia i charakter danych osobowych podlegających ochronie. Oceniając ryzyko naruszenia bezpieczeństwa danych, należy wziąć pod uwagę ryzyko cechujące przetwarzanie danych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawnio-

ny dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego oraz szkód majątkowych i niemajątkowych. Administrator i podmiot przetwarzający powinni zapewnić, by przetwarzanie danych osobowych nie było prowadzone przez osoby nieuprawnione.

(61) Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego oraz szkód majątkowych i niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą służbową lub wszelkie inne poważne szkody gospodarcze lub społeczne dla zainteresowanej osoby fizycznej. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by to naruszenie danych osobowych mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można wnieść zgłoszenia w terminie 72 godzin, powinno mu towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.

(62) Jeżeli naruszenie ochrony danych może rodzić prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych, osoby fizyczne należy poinformować bez zbędnej zwłoki, tak by mogły podjąć niezbędne środki ostrożności. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym oraz zgodnie z zaleceniami przekazanymi przez ten organ lub inne właściwe organy. Przykładowo potrzeba zmini-

malizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie. Jeżeli unikania zakłócania czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur, unikania zakłócania zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, ochrony bezpieczeństwa publicznego, ochrony bezpieczeństwa narodowego lub ochrony praw i wolności innych osób, nie można osiągnąć poprzez opóźnienie lub ograniczenie przekazania danej osobie fizycznej informacji o naruszeniu jej danych osobowych, w wyjątkowych okolicznościach można nie przekazywać takich informacji.

(63) Administrator powinien wyznaczyć osobę, która będzie pomagać mu w monitorowaniu wewnętrznego przestrzegania przepisów przyjętych na podstawie niniejszej dyrektywy, z wyjątkiem sytuacji, w której państwo członkowskie podejmie decyzję o zwolnieniu z tego obowiązku sądów i innych niezależnych organów wymiaru sprawiedliwości w toku sprawowania przez nie wymiaru sprawiedliwości. Osoba ta może być członkiem dotychczasowego personelu administratora po odbyciu specjalnego szkolenia z prawa i praktyki ochrony danych w celu uzyskania wiedzy fachowej w tej dziedzinie. Niezbędny poziom wiedzy fachowej należy ustalić zwłaszcza w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora. Swoje zadania osoba ta może wykonywać w niepełnym lub w pełnym wymiarze czasu pracy. Kilku administratorów może, uwzględniając swoją strukturę organizacyjną i wielkość, wspólnie wyznaczyć jednego inspektora ochrony danych, na przykład w przypadku dzielonych zasobów w jednostkach centralnych. Osoba ta może być również mianowana na różne stanowiska w ramach struktury poszczególnych administratorów. Osoba ta powinna pomagać administratorowi i pracownikom przetwarzającym dane osobowe, dostarczając im informacji i porad na temat przestrzegania spoczywających na nich obowiązków w zakresie ochrony

danych. Inspektorzy ochrony danych powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny, zgodnie z prawem państwa członkowskiego.

(64) Państwa członkowskie powinny zapewnić, by dane były przekazywane do państwa trzeciego lub organizacji międzynarodowej tylko wtedy, gdy jest to konieczne dla zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym dla ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz gdy administrator w państwie trzecim lub w organizacji międzynarodowej jest organem właściwym w rozumieniu niniejszej dyrektywy. Wyłącznie organy właściwe pełniące funkcję administratora powinny dokonywać przekazania, z wyjątkiem sytuacji gdy podmiotom przetwarzającym jednoznacznie polecono dokonać przekazania w imieniu administratorów. Przekazanie takie może nastąpić w przypadkach, w których Komisja zdecydowała, że dane państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, gdy wprowadzono odpowiednie zabezpieczenia lub gdy mają zastosowanie wyjątki w konkretnych sytuacjach. Przekazując dane osobowe z Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy jednak obniżać stopnia ochrony osób fizycznych przewidzianego w Unii na mocy niniejszej dyrektywy, także w przypadkach dalszego przekazywania danych osobowych z państwa trzeciego lub organizacji międzynarodowej administratorom lub podmiotom przetwarzającym w tym samym lub w innym państwie trzecim lub tej samej lub innej organizacji międzynarodowej.

(65) Przekazywanie danych osobowych z któregokolwiek państwa członkowskiego do państw trzecich lub organizacji międzynarodowych powinno zasadniczo odbywać się wyłącznie za zgodą państwa członkowskiego, od którego te dane uzyskano. Jeżeli zagrożenie dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego lub dla ważnych interesów państwa członkowskiego jest tak nagłe, że nie da się na czas uzyskać uprzedniej zgody, wtedy z uwagi na efektywność

współpracy w zakresie ścigania właściwy organ powinien móc przekazać odnośne dane osobowe do danego państwa trzeciego lub danej organizacji międzynarodowej bez takiej uprzedniej zgody. Państwa członkowskie powinny przyjąć, że należy informować państwa trzecie lub organizacje międzynarodowe o wszelkich specjalnych wymogach dotyczących przekazania. Dalsze przekazanie danych osobowych powinno podlegać uprzedniej zgodzie właściwego organu, który dokonał pierwotnego przekazania. Podejmując decyzję w sprawie wniosku o zgodę na dalsze przekazanie danych, właściwy organ, który dokonał pierwotnego przekazania, powinien odpowiednio uwzględnić wszelkie istotne czynniki, w tym wagę czynu zabronionego, szczególne warunki pierwotnego przekazania danych oraz cel tego przekazania, rodzaj i warunki wykonania kary oraz stopień ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, którym dane osobowe są dalej przekazywane. Właściwy organ, który dokonał pierwotnego przekazania, powinien także mieć możliwość uzależnienia dalszego przekazania od spełnienia szczególnych warunków. Warunki te mogą zostać opisane na przykład w kodeksach postępowania.

(66) Komisja powinna mieć możliwość stwierdzenia ze skutkiem dla całej Unii, że niektóre państwa trzecie, lub terytorium lub co najmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa, zapewniają odpowiedni stopień ochrony danych, gwarantując tym samym pewność i jednolitość prawną w całej Unii w odniesieniu do państw trzecich lub organizacji międzynarodowych, które zostały uznane za zapewniające taki stopień ochrony. W takich przypadkach powinna istnieć możliwość przekazania danych osobowych do tych państw bez konieczności uzyskania specjalnego zezwolenia, z wyjątkiem sytuacji, gdy inne państwo członkowskie, od którego uzyskano dane, musi wydać zgodę na ich przekazanie.

(67) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, w swojej ocenie państwa trzeciego lub terytorium lub określonego sektora w państwie trzecim Komisja powinna wziąć pod uwagę sposób, w jaki dane państwo trzecie

przestrzega praworządności, dostępu do wymiaru sprawiedliwości oraz międzynarodowych norm i standardów ochrony praw człowieka, jego prawo ogólne i sektorowe, w tym ustawodawstwo dotyczące bezpieczeństwa publicznego, obrony i bezpieczeństwa narodowego, a także porządku publicznego i prawa karnego. Przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do terytorium lub w określonym sektorze w państwie trzecim należy wziąć pod uwagę jasne i obiektywne kryteria, takie jak konkretne czynności przetwarzania, zakres mających zastosowanie standardów prawnych i ustawodawstwo obowiązujące w danym państwie trzecim. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi przewidzianemu w Unii, w szczególności gdy dane są przetwarzane w jednym konkretnym sektorze lub większej ich liczbie. Państwo trzecie powinno w szczególności zapewnić skuteczny niezależny nadzór nad ochroną danych oraz powinno przewidzieć mechanizmy współpracy z organami ochrony danych państw członkowskich, a osoby, których dane dotyczą, powinny uzyskać skuteczne, wykonalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia.

(68) Poza międzynarodowymi zobowiązaniami, które przyjęły państwo trzecie lub organizacja międzynarodowa, Komisja powinna brać pod uwagę także obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, zwłaszcza w odniesieniu do ochrony danych osobowych, a także realizację takich obowiązków. W szczególności powinna wziąć pod uwagę przystąpienie państwa trzeciego do Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz do Protokołu dodatkowego do tej Konwencji. Oceniając stopień ochrony w państwach trzecich lub organizacjach międzynarodowych Komisja powinna konsultować się z Europejską Radą Ochrony Danych ustanowioną rozporządzeniem (UE) 2016/679. Komisja powinna także brać pod uwagę swoje decyzje stwierdzające odpowiedni stopień ochrony przyjęte na mocy art. 45 rozporządzenia (UE) 2016/679.

(69) Komisja powinna monitorować obowiązywanie decyzji o stopniu ochrony w państwie trzecim, na terytorium lub na określonym sektorze w państwie trzecim, lub w organizacji międzynarodowej. W swoich decyzjach stwierdzających odpowiedni stopień ochrony Komisja powinna przewidzieć mechanizm okresowego przeglądu ich funkcjonowania. Takiego okresowego przeglądu Komisja powinna dokonywać w porozumieniu z danym państwem trzecim lub daną organizacją międzynarodową i powinna w nim uwzględniać wszelkie istotne zmiany w państwie trzecim lub organizacji międzynarodowej.

(70) Komisja powinna mieć również możliwość uznania, że państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony danych. W związku z tym przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej powinno zostać zakazane, chyba że spełnione są wymogi niniejszej dyrektywy dotyczące przesyłania z zastrzeżeniem odpowiednich zabezpieczeń i wyjątków w konkretnych sytuacjach. Należy przewidzieć procedury konsultacji między Komisją a takimi państwami trzecimi lub organizacjami międzynarodowymi. Komisja powinna niezwłocznie poinformować to państwo trzecie lub tę organizację międzynarodową o powodach oraz podjąć z nimi konsultacje w celu rozwiązania sytuacji.

(71) Przekazania nieprzeprowadzone na podstawie decyzji stwierdzającej odpowiedni stopień ochrony powinny być dopuszczalne jedynie wtedy, gdy w prawnie wiążącym akcie przewidziano odpowiednie zabezpieczenia zapewniające ochronę danych osobowych, lub gdy administrator ocenił wszystkie okoliczności towarzyszące przekazaniu danych i na podstawie tej oceny stwierdza, że istnieją odpowiednie zabezpieczenia w odniesieniu do ochrony danych osobowych. Takim prawnie wiążącym aktem może być przykładowo prawnie wiążąca umowa dwustronna, która została zawarta przez państwo członkowskie i wprowadzona przez nie do jego porządku prawnego, i która może być egzekwowana przez osoby, których dane dotyczą, i która zapewnia przestrzeganie wymogów ochrony danych oraz praw osób, której dane dotyczą, w tym pra-

wa do skutecznych administracyjnych lub sądowych środków zaskarżenia. Oceniając wszystkie okoliczności towarzyszące przekazaniu danych, administrator powinien mieć możliwość uwzględnienia umów o współpracy zawartych przez Europol lub Eurojust z państwami trzecimi, pozwalających na wymianę danych osobowych. Administrator powinien też mieć możliwość uwzględnienia tego, czy przekazanie danych osobowych będzie podlegać obowiązkom zachowania poufności i zasadzie ograniczonego celu, tak aby dane nie były przetwarzane do celów innych niż cele, w których zostały przekazane. Ponadto administrator powinien wziąć pod uwagę to, czy dane osobowe nie posłużą do zażądania, orzeczenia lub wykonania kary śmierci ani do innego rodzaju okrutnego lub nieludzkiego traktowania. Jakkolwiek kryteria te można uznać za odpowiednie zabezpieczenia umożliwiające przekazanie danych, administrator powinien mieć możliwość zażądania dodatkowych zabezpieczeń.

(72) Jeżeli nie wydano decyzji stwierdzającej odpowiedni stopień ochrony lub nie ma odpowiednich zabezpieczeń, przekazanie lub określona kategoria przekazań może nastąpić tylko w szczególnych sytuacjach, gdy jest to konieczne, dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, lub dla zabezpieczenia uzasadnionych prawnie interesów osoby, której dane dotyczą, zgodnie z wymogami prawa państwa członkowskiego przekazującego dane osobowe; dla zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego; w indywidualnym przypadku dla celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kary, w tym dla ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegać takim zagrożeniom; w indywidualnym przypadku dla celów ustalenia roszczenia, jego dochodzenia lub obrony. Wyjątki te należy interpretować wąsko i nie powinny one umożliwiać częstego, masowego i zorganizowanego przekazywania danych osobowych ani przekazywania danych na dużą skalę; powinny też być ograniczone do danych ściśle niezbędnych. Takie operacje przekazywania powinny być udokumentowane, a dokumentacja ta powinna być udo-

stępniana na żądanie organowi nadzorczemu w celu kontroli zgodności przekazania z prawem.

(73) Właściwe organy państw członkowskich stosują obowiązujące dwustronne lub wielostronne umowy międzynarodowe zawarte z państwami trzecimi w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, by wymieniać istotne informacje do wykonywania prawnie ciążących na nich obowiązków. Odbywa się to zasadniczo dzięki współpracy właściwych organów państw trzecich prowadzonej na potrzeby niniejszej dyrektywy, lub przynajmniej we współpracy z tymi organami, czasami nawet przy braku odpowiedniej dwustronnej lub wielostronnej umowy międzynarodowej. Niemniej w konkretnych indywidualnych przypadkach rutynowy tryb postępowania wymagający skontaktowania się z takim organem w państwie trzecim może okazać się nieskuteczny lub niewłaściwy, w szczególności ze względu na to, że przekazanie mogłoby ulec opóźnieniu, lub dlatego, że organ w państwie trzecim nie przestrzega praworządności lub międzynarodowych norm i standardów ochrony praw człowieka – w takiej sytuacji właściwe organy państw członkowskich mogą podjąć decyzję, że dane osobowe przekazane zostaną bezpośrednio odbiorcom znajdującym się w takich państwach trzecich. Może się tak zdarzyć wówczas, gdy zachodzi pilna potrzeba przekazania danych osobowych w celu ratowania życia osobie zagrożonej czynem zabronionym, lub gdy jest to konieczne do zapobieżenia spodziewanemu popełnieniu czynu zabronionego, w tym czynu terrorystycznego. Nawet jeżeli takie przekazanie między organami a odbiorcami mającymi siedzibę w państwach trzecich miałoby się odbywać tylko w konkretnych indywidualnych przypadkach, niniejsza dyrektywa powinna wskazać zasady służące uregulowaniu takich przypadków. Takich przepisów nie należy uznawać za wyjątki od obowiązujących dwustronnych lub wielostronnych umów międzynarodowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Zasady te powinny obowiązywać obok pozostałych przepisów niniejszej dyrektywy, zwłaszcza przepisów o zgodności przetwarzania z prawem i przepisów rozdziału V.

(74) Transgraniczne przekazywanie danych osobowych może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać praw do ochrony danych osobowych w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych danych. Jednocześnie organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub prowadzić postępowania w sprawie działań, która mają miejsce poza granicami ich państwa. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze oraz niespójne systemy prawne. Należy więc upowszechniać ściślejszą współpracę między organami nadzorującymi ochronę danych w celu wspierania wymiany informacji z ich zagranicznymi odpowiednikami.

(75) Zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, które mają możliwość wykonywania swych funkcji w sposób całkowicie niezależny. Organy nadzorcze powinny monitorować stosowanie niniejszej dyrektywy oraz powinny przyczyniać się do ich spójnego stosowania w całej Unii, po to by chronić osoby fizyczne w związku z przetwarzaniem jej danych osobowych. W tym celu organy nadzorcze powinny współpracować ze sobą oraz z Komisją.

(76) Odpowiedzialność za zadania, które mają być realizowane przez krajowe organy nadzorcze ustanowione na podstawie niniejszej dyrektywy, państwa członkowskie mogą powierzyć organom nadzorczym już ustanowionym na mocy rozporządzenia (UE) 2016/679.

(77) Aby odzwierciedlić swoją strukturę konstytucyjną, organizacyjną i administracyjną, państwa członkowskie powinny mieć możliwość utworzenia więcej niż jednego organu nadzorczego. Każdy organ nadzorczy powinien zostać wyposażony w zasoby finansowe i kadrowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania zadań, w tym zadań związanych z wzajemną pomocą i współpracą z innymi organami nadzorczymi z całej Unii. Każdy organ nadzorczy powinien dysponować odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.

(78) Organy nadzorcze powinny pod względem swoich wydatków finansowych podlegać niezależnym mechanizmom kontroli lub monitorowania, pod warunkiem, że taka kontrola finansowa nie wpływa na ich niezależność.

(79) Ogólne warunki członkostwa w organie nadzorczym powinny zostać określone w prawie państwa członkowskiego i powinny w szczególności zapewniać, by członków tego organu powoływał przy zastosowaniu procedury zapewniającej przejrzystość parlament, rząd lub szef danego państwa członkowskiego – na wniosek rządu, członka rządu, parlamentu lub izby parlamentu – lub niezależny organ, któremu zadanie to powierzono w prawie państwa członkowskiego. Aby zapewnić niezależność organu nadzorczego, jego członek lub członkowie powinni działać uczciwie, powstrzymać się od wszelkich czynności niezgodnych ze swoimi obowiązkami i nie powinni podczas swojej kadencji podejmować żadnego zajęcia zarobkowego ani niezarobkowego niezgodnego z tymi obowiązkami. Aby zapewnić niezależność organu nadzorczego, organ sam powinien dobierać swój personel, co może też oznaczać wybór personelu przez niezależny organ utworzony na mocy prawa państwa członkowskiego.

(80) Niniejsza dyrektywa ma zastosowanie także do działalności sądów krajowych i innych organów wymiaru sprawiedliwości, niemniej właściwość organów nadzorczych nie powinna obejmować przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości, tak by chronić niezawisłość sędziów w wykonywaniu ich zadań sądowych. Wyjątek ten należy ograniczyć do czynności sądowych w sprawach sądowych i nie powinien on mieć zastosowania do innych czynności, w których sędziowie mogą brać udział zgodnie z prawem państwa członkowskiego. Państwa członkowskie powinny mieć również możliwość przyjęcia, że właściwość organu nadzorczego nie obejmuje przetwarzania danych osobowych przez inne niezależne organy wymiaru sprawiedliwości w toku sprawowania przez nie wymiaru sprawiedliwości, przykładowo przez prokuraturę. Niemniej przestrzeganie przepisów niniejszej dyrektywy przez sądy i inne niezależne organy wymiaru sprawiedliwości zawsze podlega niezależnej kontroli zgodnie z art. 8 ust. 3 Karty.

(81) Każdy organ nadzorczy powinien rozpatrywać skargi wnoszone przez osoby, których dane dotyczą, oraz powinien zbadać taką sprawę lub przekazać ją do rozpatrzenia właściwemu organowi nadzorczemu. Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie. Organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga przeprowadzenia dalszego postępowania lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana.

(82) Aby zapewnić skuteczne, rzetelne i spójnie przestrzeganie i wykonywanie niniejszej dyrektywy w całej Unii zgodnie z TFUE w interpretacji Trybunału Sprawiedliwości, organy nadzorcze powinny mieć w każdym państwie członkowskim te same zadania i faktyczne uprawnienia, w tym uprawnienia w zakresie prowadzenia postępowań, uprawnienia naprawcze i doradcze, które umożliwiają wykonywanie powierzonych im zadań. Ich uprawnienia nie powinny jednak kolidować ze szczegółowymi przepisami postępowania karnego, w tym o prowadzeniu postępowań przygotowawczych i ściganiu czynów zabronionych, ani z niezawisłością sądów. Z zastrzeżeniem uprawnień organów prokuratorskich na mocy prawa państwa członkowskiego organy nadzorcze powinny również mieć uprawnienie do wnoszenia naruszeń niniejszej dyrektywy przed organy sądowe lub do udziału w postępowaniu sądowym. Ze swoich uprawnień organ nadzorczy powinien korzystać zgodnie z odpowiednimi gwarancjami proceduralnymi przewidzianymi w prawie Unii i w prawie państwa członkowskiego, bezstronnie, sprawiedliwie i w rozsądnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny do zapewnienia przestrzegania niniejszej dyrektywy, z uwzględnieniem okoliczności danej sprawy, poszanowania prawa wysłuchania danej osoby przed zastosowaniem indywidualnego środka, który miałby niekorzystnie na nią wpłynąć, i bez nadmiernych kosztów i niedogodności dla danej osoby. Z uprawnień w zakresie prowadze-

nia postępowań wyjaśniających, jeżeli chodzi o dostęp do pomieszczeń, należy korzystać zgodnie ze szczegółowymi wymogami prawa państwa członkowskiego, takimi jak wymóg uzyskania wcześniejszej zgody sądu. Wydanie prawnie wiążącej decyzji powinno podlegać kontroli sądowej w państwie członkowskim organu nadzorczego, który ją wydał.

(83) Organy nadzorcze powinny wspierać się wzajemnie w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i wykonanie przepisów przyjętych na podstawie niniejszej dyrektywy.

(84) Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania niniejszej dyrektywy w całej Unii, w tym poprzez doradzanie Komisji i propagowanie współpracy organów nadzorczych w całej Unii.

(85) Każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka prawnego przed sądem zgodnie z art. 47 Karty praw podstawowych, jeżeli uzna, że jej prawa wynikające z przepisów przyjętych na podstawie niniejszej dyrektywy są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, w części lub w całości ją odrzuca lub oddala lub nie podejmuje działania, choć jest ono niezbędne do ochrony praw osoby, której dane dotyczą. Postępowanie wyjaśniające w sprawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiednim do konkretnej sprawy. Właściwy organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga przeprowadzenia dalszego postępowania wyjaśniającego lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana. Aby ułatwić wnoszenie skarg, każdy organ nadzorczy powinien przedsięwziąć takie środki, jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji.

(86) Każda osoba fizyczna lub prawna powinna mieć prawo do skutecznego środka prawnego przed właściwym sądem krajowym od decyzji organu nadzorczego wywołującej skutki prawne wobec tej osoby. Taka decyzja może dotyczyć zwłaszcza wykonywania przez organ nadzorczy uprawnień do prowadzenia postępowań wyjaśniających, uprawnień naprawczych i do wydawania zezwoleń lub oddalania lub odrzucania skarg. Prawo to nie dotyczy jednak innych niewiążących prawnie środków organów nadzorczych, takich jak wydawane przez organ opinie czy zalecenia. Postępowanie przeciwko organowi nadzorczemu należy wszcząć przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę, a postępowanie powinno się toczyć zgodnie z prawem tego państwa członkowskiego. Sądy te powinny wykonywać pełną jurysdykcję w sprawie, w tym w zakresie ustalenia okoliczności faktycznych i prawnych istotnych dla rozstrzygnięcia sprawy.

(87) Jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z niniejszej dyrektywy, powinna mieć prawo do umocowania podmiotu – którego celem jest ochrona praw i interesów osób w odniesieniu do ochrony jej danych osobowych oraz który został ustanowiony zgodnie z prawem państwa członkowskiego – do wniesienia skargi w swoim imieniu do organu nadzorczego oraz do wykonania prawa do środka prawnego przed sądem. Prawo osoby, której dane dotyczą, do reprezentacji nie powinno uchybiać prawu procesowemu państwa członkowskiego, które może wymagać, by osoba, której dane dotyczą, była przed sądami krajowymi obowiązkowo reprezentowana przez prawnika w rozumieniu dyrektywy Rady 77/249/EWG[10].

(88) Za wszelką szkodę, którą dana osoba mogła ponieść wskutek przetwarzania z naruszeniem przepisów przyjętych na podstawie niniejszej dyrektywy, powinno przysługiwać odszkodowanie od administratora lub innego organu właściwego w świetle prawa państwa członkowskiego. Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Try-

[10] Dyrektywa Rady 77/249/EWG z dnia 22 marca 1977 r. mająca na celu ułatwienie skutecznego korzystania przez prawników ze swobody świadczenia usług (Dz.U. L 78 z 26.3.1977, s. 17).

bunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszej dyrektywy. Nie ma to wpływu na jakiekolwiek roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego. W przypadku odwołania do przetwarzania niezgodnego z prawem lub z naruszeniem przepisów przyjętych na podstawie niniejszej dyrektywy, odwołanie obejmuje także przetwarzanie, które narusza akty wykonawcze przyjęte na podstawie niniejszej dyrektywy. Osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesioną szkodę.

(89) Każda osoba fizyczna lub prawna, niezależnie od tego czy działa na podstawie prawa prywatnego czy publicznego, która narusza niniejszą dyrektywę, powinna podlegać sankcjom. Państwa członkowskie powinny zapewnić, by sankcje były skuteczne, proporcjonalne i odstraszające, oraz powinny podjąć wszelkie środki służące wykonaniu sankcji.

(90) Aby zapewnić jednolite warunki wdrażania niniejszej dyrektywy, należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do: stwierdzania odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizację międzynarodową; określania formuły i trybu wzajemnej pomocy oraz ustalania zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[11].

(91) Należy stosować procedurę sprawdzającą dla przyjmowania aktów wykonawczych w sprawie stwierdzenia odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizację międzynarodową oraz w sprawie formuły i trybu wzajemnej pomocy i ustalania zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

organami nadzorczymi a Europejską Radą Ochrony Danych, zważywszy, że akty te mają zasięg ogólny.

(92) Komisja powinna przyjmować akty wykonawcze o natychmiastowym zastosowaniu, jeżeli jest to szczególnie pilne w należycie uzasadnionych przypadkach, dotyczących państwa trzeciego, terytorium lub określonego sektora w państwie trzecim, lub organizacji międzynarodowej, które nie zapewniają dłużej odpowiedniego stopnia ochrony.

(93) Ponieważ cele niniejszej dyrektywy – którymi są ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych, oraz zapewnienie swobodnego przepływu danych osobowych między właściwymi organami w ramach całej Unii – nie mogą w wystarczającym stopniu zostać osiągnięte przez państwa członkowskie, natomiast z uwagi na zakres i skutki działania możliwe jest lepsze ich osiągnięcie na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym samym artykule niniejsza dyrektywa nie wykracza poza zakres niezbędny do osiągnięcia tych celów.

(94) Dyrektywa nie powinna wpływać na szczegółowe przepisy aktów unijnych przyjętych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, które zostały przyjęte przed datą przyjęcia niniejszej dyrektywy i regulują przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów – przepisy takie, jak np. szczegółowe przepisy o ochronie danych osobowych stosowane na mocy decyzji Rady 2008/615/WSiSW[12] czy art. 23 Konwencji o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej[13]. Jako

[12] Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 1).

[13] Akt Rady z dnia 29 maja 2000 r. ustanawiający zgodnie z art. 34 Traktatu o Unii Europejskiej Konwencję o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (Dz.U. C 197 z 12.7.2000, s. 1).

że zgodnie z art. 8 Karty i art. 16 TFUE prawo podstawowe do ochrony danych osobowych powinno być spójnie stosowane w całej Unii, Komisja powinna ocenić sytuację pod kątem stosunku niniejszej dyrektywy do aktów, które zostały przyjęte przed datą przyjęcia niniejszej dyrektywy i regulują przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów, oraz ustalić, czy należy te szczegółowe przepisy dostosować do niniejszej dyrektywy. W razie potrzeby Komisja powinna przedstawić wnioski celem zapewnienia spójności przepisów dotyczących przetwarzania danych osobowych.

(95) Aby ochrona danych osobowych w Unii była kompleksowa i spójna, międzynarodowe porozumienia, które zostały zawarte przez państwa członkowskie przed wejściem niniejszej dyrektywy w życie i które są zgodne z odnośnym prawem Unii mającym zastosowanie przed tą datą, powinny pozostać w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

(96) Na transponowanie niniejszej dyrektywy państwom członkowskim należy przyznać nie więcej niż dwa lata od dnia jej wejścia w życie. Przetwarzanie, które w tym dniu jest w toku, powinno w terminie dwóch lat od dnia wejścia w życie niniejszej dyrektywy zostać dostosowane do jej przepisów. Jeżeli jednak takie przetwarzanie jest zgodne z prawem Unii mającym zastosowanie przed dniem wejścia niniejszej dyrektywy w życie, wymogi niniejszej dyrektywy dotyczące uprzednich konsultacji z organem nadzorczym nie powinny mieć zastosowania do operacji przetwarzania, które już ma miejsce, gdyż z uwagi na ich charakter wymogi te powinny zostać spełnione przed przetwarzaniem. Jeżeli państwa członkowskie stosują dłuższy termin wdrożenia, upływający siedem lat po dniu wejścia niniejszej dyrektywy w życie, dla wypełnienia zobowiązań dotyczących ewidencjonowania w zautomatyzowanych systemach przetwarzania ustanowionych przed tą datą, administrator lub podmiot przetwarzający powinni dysponować skutecznymi metodami, które pozwolą im na wykazanie zgodności przetwarzania danych z prawem, monitorowanie własnej działalności i zapewnienie integralności i bezpieczeństwa danych, takimi jak ewidencja lub inne formy zapisu.

(97) Niniejsza dyrektywa nie wpływa na przepisy o zwalczaniu niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz o zwalczaniu pornografii dziecięcej ustanowione w dyrektywie 2011/93/UE Parlamentu Europejskiego i Rady[14].

(98) Należy zatem uchylić decyzję ramową 2008/977/WSiSW.

(99) Zgodnie z art. 6a Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który jest załączony do TUE i TFUE, Zjednoczone Królestwo i Irlandia nie są związane przepisami ustanowionymi w niniejszej dyrektywie, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, jeżeli państwa te nie są związane zasadami regulującymi formy współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, w ramach której należy przestrzegać przepisów ustanowionych na podstawie art. 16 TFUE.

(100) Zgodnie z art. 2 i 2a Protokołu nr 22 w sprawie stanowiska Danii, który jest załączony do TUE i TFUE, Dania nie jest związana przepisami ustanowionymi w niniejszej dyrektywie ani im nie podlega, o ile przepisy te dotyczą przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE. Ponieważ niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu części trzeciej tytuł V TFUE, Dania zgodnie z art. 4 tego Protokołu podejmie w terminie sześciu miesięcy od daty przyjęcia niniejszej dyrektywy decyzję, czy dokona jej transpozycji do swojego prawa krajowego.

[14] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. L 335 z 17.12.2011, s. 1).

(101) W odniesieniu do Islandii i Norwegii niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[15].

(102) W odniesieniu do Szwajcarii niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[16].

(103) W odniesieniu do Liechtensteinu niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[17].

(104) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w Karcie umocowanej TFUE, w szczególności z prawem do poszanowania życia prywatnego i rodzinnego, prawem do ochrony danych osobowych oraz prawem do skutecznego środka prawnego i do rzetelnego procesu. Ograniczenia tych praw są zgodne z art. 52 ust. 1 Karty, ponieważ są niezbędne do realizacji celów leżących w interesie ogólnym i uznanych przez Unię lub do ochrony praw i wolności innych osób.

(105) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji z dnia 28 września 2011 r. dotyczącą dokumentów wyjaśniających państwa członkowskie zobowiązały się w uzasadnionych przypadkach dołączać do zawiadomienia o swoich środkach transpozycji

[15] Dz.U. L 176 z 10.7.1999, s. 36.
[16] Dz.U. L 53 z 27.2.2008, s. 52.
[17] Dz.U. L 160 z 18.6.2011, s. 21.

przynajmniej jeden dokument wyjaśniający związek między elementami dyrektywy a odpowiadającymi im częściami krajowych środków transpozycyjnych. W odniesieniu do niniejszej dyrektywy prawodawca uznaje przekazywanie takich dokumentów za uzasadnione.

(106) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 przeprowadzono konsultację z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 7 marca 2012 r. [18]

(107) Niniejsza dyrektywa nie powinna uniemożliwiać państwom członkowskim wykonywania praw osób, których dane dotyczą, do informacji, dostępu i do sprostowania lub usunięcia danych osobowych oraz ograniczenia przetwarzania w toku postępowania karnego, oraz ewentualnych ograniczeń tych praw, w krajowych przepisach procedury karnej,

PRZYJMUJE NINIEJSZĄ DYREKTYWĘ:

[18] Dz.U. C 192 z 30.6.2012, s. 7.

ODO 24

Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

Pomożemy osiągnąć zgodność z DODO

- **Szkolenia** pracowników w formacie:
  - szkoleń zamkniętych (od 2000 zł),
  - szkoleń otwartych (od 650 zł/os.),
  - e-lerningu (od 60 zł/os.).
- **Przygotowanie** lub weryfikację dokumentacji ochrony danych.
- **Bieżące wsparcie** wyznaczonego inspektora ochrony danych.

ODO24.pl/DODO tel. **22 740 99 00**

Do każdego szkolenia stacjonarnego i pakietu e-learningowego oferujemy **GRATIS** komentarz do ustawy DODO.