Dz. U. 2019 poz. 125

Opracowano na podstawie: t.j. Dz. U. z 2023 r. poz. 1206.

U S T A W A

z dnia 14 grudnia 2018 r.

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

Rozdział 1

Przepisy ogólne

Art. 1. Ustawa określa:

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

[1)] Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89).

6) sposób zabezpieczenia danych osobowych;
7) tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej;
8) odpowiedzialność karną za naruszenie przepisów niniejszej ustawy.

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

Art. 3. Przepisów ustawy nie stosuje się do ochrony danych osobowych:
1) znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2023 r. poz. 127 oraz z 2022 r. poz. 2600), ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2022 r. poz. 1375, 1855, 2582 i 2600 oraz z 2023 r. poz. 289 i 535), ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2023 r. poz. 654), ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2022 r. poz. 1124), 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 2022 r. poz. 1689), ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2022 r. poz. 1247, 1259 i 2582 oraz z 2023 r. poz. 240), ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich (Dz. U. poz. 1700 oraz z 2023 r. poz. 289);
2) przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego.

Art. 4. Ilekroć w ustawie jest mowa o:
1) administratorze – rozumie się przez to właściwy organ, który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala

cele i sposoby przetwarzania danych osobowych, podmiot wskazany przez ustawę jako administrator, jeżeli cele i sposoby przetwarzania danych osobowych są określone w ustawie, albo podmiot wskazany przez prawo Unii Europejskiej albo prawo państwa członkowskiego Unii Europejskiej lub podmiot wyznaczony zgodnie z kryteriami określonymi w prawie tego państwa;

2) danych biometrycznych – rozumie się przez to dane osobowe dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, w tym wizerunek twarzy lub dane daktyloskopijne, które zostały uzyskane wskutek specjalnego przetwarzania technicznego;

3) danych dotyczących zdrowia – rozumie się przez to dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym dane o korzystaniu z usług opieki zdrowotnej, które ujawniają informacje o stanie jej zdrowia;

4) danych genetycznych – rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które zostały uzyskane w szczególności z analizy próbki biologicznej pochodzącej od tej osoby;

5) danych osobowych – rozumie się przez to dane osobowe, o których mowa w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[2)]);

6) naruszeniu ochrony danych osobowych – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub

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

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 przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
16) właściwym organie – rozumie się przez to organ władzy publicznej, jednostkę organizacyjną lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych;
17) zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rozdział 2

Zadania organu nadzorczego

Art. 5. 1. Do zadań Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu”, należy:
1) monitorowanie i egzekwowanie stosowania przepisów niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych;
2) upowszechnianie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych w celu, o którym mowa w art. 1 pkt 1;
3) doradzanie instytucjom publicznym w sprawach środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych w celu, o którym mowa w art. 1 pkt 1;

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

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

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

Art. 6. W celu wykonania zadań, o których mowa w art. 5 ust. 1 pkt 1 i 6–8, Prezes Urzędu może przeprowadzać kontrolę przetwarzania danych osobowych, zwaną dalej „kontrolą”. Do prowadzenia kontroli stosuje się odpowiednio przepisy rozdziału 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), z wyłączeniem art. 79 ust. 1 pkt 2, art. 83, art. 84 ust. 4 i art. 85 tej ustawy.

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

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

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

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

3. Decyzje Prezesa Urzędu, o których mowa w ust. 2, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Administrator

w przypadku uznania, że zgromadzone w ten sposób dane są zbędne, jest obowiązany do ich usunięcia. W przypadku niedopełnienia obowiązku usunięcia danych osobowych przez administratora Prezes Urzędu może nakazać ich usunięcie. W celu realizacji uprawnienia Prezes Urzędu nie uzyskuje dostępu do danych osobowych, o których mowa w zdaniu pierwszym. Administrator lub podmiot przetwarzający dane osobowe, o których mowa w zdaniu pierwszym, jest obowiązany do niezwłocznego przywrócenia zgodnego z prawem sposobu ich przetwarzania.

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

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

Art. 10. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1 pkt 5 i 9, Prezes Urzędu może kierować do administratora lub podmiotu przetwarzającego wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych zbieranych w celach, o których mowa w art. 1 pkt 1.

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

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

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

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

Art. 12. Do postępowań w sprawach objętych zakresem regulacji niniejszego rozdziału stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks

postępowania administracyjnego (Dz. U. z 2023 r. poz. 775), zwanej dalej „Kodeksem postępowania administracyjnego”, o ile przepisy niniejszej ustawy nie stanowią inaczej.

Rozdział 3

Zasady dotyczące przetwarzania danych osobowych

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

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

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

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

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

Art. 14. 1. Niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej, zwanych dalej „danymi wrażliwymi”.

2. Dopuszcza się przetwarzanie danych wrażliwych, jeżeli:

1) przepisy prawa zezwalają na ich przetwarzanie lub

2) jest to niezbędne dla ochrony życia lub zdrowia lub interesów osoby, której dane dotyczą, lub innej osoby, lub
3) dane takie zostały upublicznione przez osobę, której dotyczą.

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

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

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

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

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

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

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

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

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

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

Art. 21. 1. Właściwy organ może 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, niezbędne 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

Art. 22. 1. Administrator udostępnia informacje o:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Art. 25. 1. Jeżeli:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić,

2) dane osobowe, które podlegają usunięciu, muszą zostać zachowane do celów dowodowych

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

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

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe, lub w sprawach, o których mowa w art. 359 ust. 1 ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich;
4) zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
5) zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
6) istotne naruszenie dóbr osobistych innych osób.

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

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

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

Art. 29. Administrator w przypadku, o którym mowa w art. 26 ust. 1, poucza osobę, której dane dotyczą, o możliwości wniesienia skargi do Prezesa Urzędu w sposób określony w art. 30 ust. 2.

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

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

3. Administrator, bez zbędnej zwłoki, informuje pisemnie w postaci papierowej lub elektronicznej lub za pośrednictwem środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344) osobę, której dane dotyczą, o działaniach podjętych w związku z jej wnioskiem lub, jeżeli to możliwe, udziela wnioskowanych informacji.

4. Komunikacja prowadzona przez administratora z osobą, której dane dotyczą, na podstawie art. 15, art. 22–25 i art. 45 jest wolna od opłat. Jeżeli żądania

osoby, której dane dotyczą, są nieuzasadnione lub nadmierne, zwłaszcza ze względu na ich powtarzalność, administrator może:

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

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

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

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

Rozdział 5

Administrator i podmiot przetwarzający

Oddział 1

Przepisy ogólne

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

1) przetwarzane zgodnie z prawem i rzetelnie oraz przy zastosowaniu niezbędnych środków technicznych i organizacyjnych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
2) przetwarzane w konkretnych i uzasadnionych celach;
3) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;

5) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczone przed ich udostępnieniem osobom nieupoważnionym lub wejściem w posiadanie przez osobę nieuprawnioną.

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

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

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

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

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

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

Art. 32. 1. Administrator, w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, stosuje odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, które zostały zaprojektowane w celu skutecznej realizacji zasad ochrony danych osobowych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak aby

spełnić wymogi niniejszej ustawy, chroniły prawa osób, których dane dotyczą, oraz uwzględniały stan wiedzy technicznej, koszt wdrożenia i charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia wynikające z przetwarzania.

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

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

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

2. Współadministratorzy:

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

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

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

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

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

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

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

5. Podmiot przetwarzający jest zobowiązany:

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

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

6. Podmiot przetwarzający może powierzyć przetwarzanie danych innemu podmiotowi przetwarzającemu każdorazowo wyłącznie na podstawie pisemnej

umowy, w przypadku gdy umowa, o której mowa w ust. 1, przewiduje takie prawo, na warunkach i w zakresie przez nią określonym.

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

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

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

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

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

8) planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe;
9) ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych, o których mowa w art. 39, jeżeli jest to możliwe.

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

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

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

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

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

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

2. Ewidencjonowaniu podlegają operacje przetwarzania, w szczególności:

1) zbieranie;
2) modyfikowanie;
3) przeglądanie;
4) ujawnianie wraz z przekazywaniem;

5) łączenie;

6) usuwanie.

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

1) datę i godzinę operacji;

2) tożsamość osoby, która przeglądała lub ujawniła dane osobowe – w miarę możliwości;

3) tożsamość odbiorców danych osobowych – w miarę możliwości.

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

5. Ewidencje obejmujące czynności przetwarzania są przeznaczone wyłącznie:

1) do weryfikacji zgodności przetwarzania z prawem;

2) do monitorowania własnej działalności;

3) dla zapewnienia integralności i bezpieczeństwa danych osobowych;

4) na potrzeby postępowania karnego.

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

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

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

1) ogólny opis planowanych operacji przetwarzania danych osobowych;

2) ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą;

3) środki planowane w celu rozwiązania takiego ryzyka;

4) zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazanie zgodności z niniejszą ustawą.

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

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

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

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

3. Administrator przedstawia Prezesowi Urzędu:

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

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

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

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

Oddział 2

Zabezpieczenie danych osobowych

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

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

10) zapewnienie działania funkcji systemu, zgłaszania występujących w nich błędów (niezawodność) oraz odporności przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

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

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

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

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

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

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

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

1) imię i nazwisko osoby upoważnionej;

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

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

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

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

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

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

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

1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wykazów danych osobowych, których dotyczy naruszenie;
2) imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, który może udzielić dodatkowych informacji;

3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
4) opis środków zastosowanych lub zaproponowanych przez administratora w celu usunięcia naruszenia ochrony danych osobowych, w tym zminimalizowania jego ewentualnych negatywnych skutków.

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

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

7. W przypadku gdy naruszenie ochrony danych osobowych dotyczyło danych osobowych:
1) otrzymanych od administratora innego państwa członkowskiego Unii Europejskiej,
2) przesłanych do administratora innego państwa członkowskiego Unii Europejskiej

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

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

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

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

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, jeżeli został spełniony jeden z poniższych warunków:
1) administrator zastosował odpowiednie techniczne i organizacyjne środki ochrony, w szczególności szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wskazanych w ust. 1;
3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku.

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

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

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

Oddział 3

Inspektor ochrony danych

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

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

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

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

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

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

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

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

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

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

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

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

1) informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;

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

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

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

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb i sposób realizacji zadań, o których mowa w ust. 1, uwzględniając konieczność zapewnienia

prawidłowości realizacji zadań inspektora ochrony danych oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.

Rozdział 6

Współpraca z organami nadzorczymi w innych państwach Unii Europejskiej

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

2. Wniosek o pomoc dotyczy w szczególności:

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział 7

Środki ochrony prawnej i odpowiedzialność prawna

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

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

3. Skargę można wnieść za pomocą formularza zamieszczonego 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.

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

2. Każdej osobie, której dane dotyczą, przysługuje prawo do wniesienia do sądu administracyjnego skargi, jeżeli Prezes Urzędu nie rozpatrzył skargi lub zgłoszenia wniesionego na mocy art. 50 lub nie poinformował osoby, której dane dotyczą, w terminie 3 miesięcy od dnia wpływu skargi, o 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 2023 r. poz. 259), z tym że:

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

Art. 52. Osoba, której dane dotyczą, może umocować organizację społeczną o charakterze niezarobkowym, prowadzącą działalność statutową w interesie publicznym i działającą w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych – do wykonywania w jej imieniu praw, w tym wnoszenia środków zaskarżenia określonych w niniejszym rozdziale.

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

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

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

4. W przypadku przystąpienia Prezesa Urzędu do toczącego się postępowania przed sądem stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2021 r. poz. 1805, z późn. zm.[3)]) o interweniencie ubocznym.

Rozdział 8

Przepisy karne

Art. 54. 1. Kto przetwarza dane osobowe, o których mowa w przepisach o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

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

Art. 55. Kto udaremnia lub istotnie utrudnia kontrolującemu przeprowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości,

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 1981, 2052, 2262, 2270, 2289, 2328 i 2459, z 2022 r. poz. 1, 366, 480, 807, 830, 974, 1098, 1301, 1371, 1692, 1855, 1967, 2127, 2140, 2180, 2339, 2436, 2600 i 2687 oraz z 2023 r. poz. 289, 326, 403, 535, 556, 614 i 739.

podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat dwóch.

Rozdział 9

Zmiany w przepisach

Art. 56–97. (pominięte)[4)]

Rozdział 10

Przepisy przejściowe, dostosowujące i końcowe

Art. 98. 1. Osoba pełniąca w dniu wejścia w życie niniejszej ustawy funkcję inspektora ochrony danych osobowych na podstawie przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669), staje się inspektorem ochrony danych i pełni swoją funkcję nie dłużej jednak niż 3 miesiące od dnia wejścia w życie niniejszej ustawy, chyba że przed tym dniem administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na inspektora ochrony danych, w sposób określony w art. 46.

2. Osoba, która stała się inspektorem ochrony danych na podstawie ust. 1, pełni swoją funkcję także po upływie 3 miesięcy od dnia wejścia w życie niniejszej ustawy, jeżeli do tego dnia administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o jej wyznaczeniu, w sposób określony w art. 46.

3. Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał inspektora ochrony danych osobowych, o którym mowa w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, jest obowiązany do wyznaczenia inspektora ochrony danych i zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu, w terminie 1 miesiąca od dnia wejścia w życie niniejszej ustawy.

Art. 99. 1. Do kontroli wszczętych na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723) i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

[4)] Zamieszczone w obwieszczeniu Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 11 maja 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. poz. 1206).

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

Art. 100. 1. Postępowania prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych, wszczęte i niezakończone przed dniem wejścia w życie niniejszej ustawy, prowadzone są na podstawie przepisów dotychczasowych.

2. Czynności dokonane w postępowaniach, o których mowa w ust. 1, pozostają skuteczne, o ile zostały dokonane zgodnie z przepisami obowiązującymi w czasie ich dokonywania.

3. W przypadku wniesienia przed dniem wejścia w życie niniejszej ustawy, na podstawie art. 21 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wniosku o ponowne rozpatrzenie sprawy, będące w toku postępowanie wszczęte tym wnioskiem umarza się z mocy prawa z dniem wejścia w życie niniejszej ustawy.

4. Stronę, która zainicjowała postępowanie, o którym mowa w ust. 3, organ poucza o prawie złożenia do sądu administracyjnego skargi na decyzję, od której strona złożyła wniosek o ponowne rozpatrzenie sprawy.

5. Termin na wniesienie skargi w przypadku, o którym mowa w ust. 4, wynosi 3 miesiące od dnia doręczenia pouczenia. Do czasu upływu tego terminu decyzja, od której strona złożyła wniosek o ponowne rozpatrzenie sprawy, nie podlega wykonaniu.

Art. 101. Podmiot, do którego przed dniem wejścia w życie niniejszej ustawy zostało skierowane wystąpienie lub wniosek, o których mowa w art. 19a ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jest obowiązany przekazać Prezesowi Urzędu Ochrony Danych Osobowych odpowiedź na wystąpienie lub wniosek, na piśmie, w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

Art. 102. 1. W terminie 1 roku od dnia wejścia w życie niniejszej ustawy administrator dostosowuje zasady przetwarzania danych osobowych do środków technicznych i organizacyjnych, o których mowa w art. 39.

2. Jeżeli wymaga to niewspółmiernie dużego wysiłku lub nakładów, administrator może dostosować zautomatyzowane systemy przetwarzania danych

osobowych do środków technicznych i organizacyjnych, w terminie dłuższym niż wskazany w ust. 1, nie później jednak niż do dnia 6 maja 2023 r.

3. Dotychczasowe rozstrzygnięcia określające zasady udostępniania informacji i danych osobowych z Centralnej Bazy Danych Osób Pozbawionych Wolności, za pośrednictwem systemu teleinformatycznego, zachowują moc do dnia wejścia w życie decyzji wydanych na podstawie art. 25d ust. 1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, nie dłużej jednak niż przez okres 2 lat od dnia wejścia w życie niniejszej ustawy.

4. Dostosowanie zasad przetwarzania informacji i danych osobowych w zbiorach danych utworzonych przed dniem wejścia w życie niniejszej ustawy do wymogów, o których mowa w art. 19, art. 20 i art. 36, nastąpi nie później niż do dnia 6 maja 2023 r.

Art. 103. Wydane przed dniem wejścia w życie ustawy upoważnienia do przetwarzania danych osobowych zachowują moc przez okres 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 104. Zgody wydane przez służby, instytucje państwowe oraz organy władzy publicznej na udostępnianie za pomocą urządzeń telekomunikacyjnych lub w drodze teletransmisji informacji, w tym danych osobowych, jednostkom organizacyjnym Policji, jednostkom organizacyjnym Straży Granicznej, Służbie Ochrony Państwa oraz organom Krajowej Administracji Skarbowej zachowują swoją moc, z zastrzeżeniem art. 102 ust. 3.

Art. 105. Dotychczasowe przepisy wykonawcze wydane na podstawie:

1) art. 15 ust. 8 i art. 20 ust. 19 ustawy zmienianej w art. 58,
2) art. 10a ust. 8 i art. 11 ust. 2 ustawy zmienianej w art. 59,
3) art. 25 ust. 3 ustawy zmienianej w art. 80,
4) art. 29 ust. 8 ustawy zmienianej w art. 72,
5) art. 42 ust. 6 ustawy zmienianej w art. 81,
6) art. 10 ustawy zmienianej w art. 85

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

1) art. 15 ust. 8, art. 20 ust. 1n i art. 20 ust. 1o ustawy zmienianej w art. 58, w brzmieniu nadanym niniejszą ustawą,

2) art. 10a ust. 18 i art. 11 ust. 2 ustawy zmienianej w art. 59, w brzmieniu nadanym niniejszą ustawą,
3) art. 25 ust. 3 ustawy zmienianej w art. 80, w brzmieniu nadanym niniejszą ustawą,
4) art. 29 ust. 17 ustawy zmienianej w art. 72, w brzmieniu nadanym niniejszą ustawą,
5) art. 42 ust. 6 ustawy zmienianej w art. 81, w brzmieniu nadanym niniejszą ustawą,
6) art. 10 ustawy zmienianej w art. 85, w brzmieniu nadanym niniejszą ustawą

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

Art. 106. 1. Maksymalny limit wydatków z budżetu państwa przeznaczonych na wykonywanie zadań wynikających z niniejszej ustawy wynosi w:

1) 2019 r. – 1 250 000 zł;
2) 2020 r. – 1 350 000 zł;
3) 2021 r. – 1 380 000 zł;
4) 2022 r. – 1 410 000 zł;
5) 2023 r. – 1 450 000 zł;
6) 2024 r. – 1 490 000 zł;
7) 2025 r. – 1 530 000 zł;
8) 2026 r. – 1 570 000 zł;
9) 2027 r. – 1 610 000 zł;
10) 2028 r. – 1 650 000 zł.

2. Prezes Urzędu Ochrony Danych Osobowych monitoruje wykorzystanie limitu wydatków, o których mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału. Ocena za IV kwartał jest dokonywana według stanu na dzień 20 listopada danego roku.

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

mechanizm korygujący polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym niniejszej ustawy.

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

Art. 107. Tracą moc art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziały 4, 5 i 7 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych zachowane w mocy w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz 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.

Art. 108. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia[5)], 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.

5) Ustawa została ogłoszona w dniu 22 stycznia 2019 r.