# Ustawa o ochronie danych osobowych

1)2)

**z dnia 29 sierpnia 1997 r. (Dz.U. Nr 133, poz. 883)**

**tj. z dnia 17 czerwca 2002 r. (Dz.U. Nr 101, poz. 926)**

**tj. z dnia 26 czerwca 2014 r. (Dz.U. z 2014 r. poz. 1182)**

**tj. z dnia 25 listopada 2015 r. (Dz.U. z 2015 r. poz. 2135)**

**tj. z dnia 13 czerwca 2016 r. (Dz.U. z 2016 r. poz. 922)**

(zm. Dz.U. z 2018 r. poz. 1000, Dz.U. z 2018 r. poz. 138)

## Rozdział 1. Przepisy ogólne.

**Art. 1 [Prawo do ochrony]**
1. Każdy ma prawo do ochrony dotyczących go danych osobowych.
2. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą.

**Art. 2 [Przedmiot regulacji]**
1. Ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.
2. Ustawę stosuje się do przetwarzania danych osobowych:
**1)** w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych;
**2)** w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.
3. W odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5.

**Art. 3 [Zakres stosowania]**
1. Ustawę stosuje się do organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych.
2. *(utracił moc)*

**Art. 3a** ***(utracił moc)***

**Art. 4 [Wyłączenie stosowania]** Przepisów ustawy nie stosuje się, jeżeli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej.

**Art. 5 [Odesłanie]** Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

**Art. 6 [Objaśnienia]**
1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

**Art. 7 [Słowniczek]** Ilekroć w ustawie jest mowa o:
**1)** zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
**2)** przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
**2a)** systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
**2b)** zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
**3)** usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
**4)** administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych;
**5)** zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;
**6)** odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
- **a)** osoby, której dane dotyczą,
- **b)** osoby upoważnionej do przetwarzania danych,
- **c)** przedstawiciela, o którym mowa w art. 31a,
- **d)** podmiotu, o którym mowa w art. 31,
- **e)** organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

**7)** państwie trzecim - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

## Rozdział 2. Organ ochrony danych osobowych.

**Art. 8** *(utracił moc)*
**Art. 9** *(utracił moc)*
**Art. 10** *(utracił moc)*
**Art. 11** *(utracił moc)*
**Art. 11a** *(utracił moc)*
**Art. 11b** *(utracił moc)*
**Art. 11c** *(utracił moc)*
**Art. 11d** *(utracił moc)*
**Art. 11e** *(utracił moc)*
**Art. 11f** *(utracił moc)*
**Art. 11g** *(utracił moc)*
**Art. 12** *(utracił moc)*
**Art. 12a** *(utracił moc)*
**Art. 13** *(utracił moc)*

**Art. 14 [Uprawnienia inspektorów]** W celu wykonania zadań, o których mowa w art. 12 pkt 1 i 2, Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura, zwani dalej "inspektorami", mają prawo:
1) wstępu, w godzinach od $6^{00}$ do $22^{00}$, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
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 urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych;
5) zlecać sporządzanie ekspertyz i opinii.

**Art. 15 [Umożliwienie kontroli]**
1. Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności oraz spełnić żądania, o których mowa w art. 14 pkt 1-4.
2. W toku kontroli zbiorów, o których mowa w art. 43 ust. 1 pkt 1a, inspektor przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej.
3. Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową.
4. Imienne upoważnienie powinno zawierać:
1) wskazanie podstawy prawnej przeprowadzenia kontroli;
2) oznaczenie organu kontroli;
3) imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli oraz numer jej legitymacji służbowej;
4) określenie zakresu przedmiotowego kontroli;
5) oznaczenie podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli;
6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia kontroli;
7) podpis Generalnego Inspektora;
8) pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach;
9) datę i miejsce wystawienia imiennego upoważnienia.

**Art. 16 [Protokół z czynności kontrolnych]**
1. Z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu administratorowi danych.
1a. Protokół kontroli powinien zawierać:
1) nazwę podmiotu kontrolowanego w pełnym brzmieniu i jego adres;
2) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia inspektora;
3) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
4) datę rozpoczęcia i zakończenia czynności kontrolnych, z wymienieniem dni przerw w kontroli;
5) określenie przedmiotu i zakresu kontroli;
6) opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) wyszczególnienie załączników stanowiących składową część protokołu;
8) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;
9) parafy inspektora i osoby reprezentującej podmiot kontrolowany na każdej stronie protokołu;
10) wzmiankę o doręczeniu egzemplarza protokołu osobie reprezentującej podmiot kontrolowany;
11) wzmiankę o wniesieniu lub niewniesieniu zastrzeżeń i uwag do protokołu;

12) datę i miejsce podpisania protokołu przez inspektora oraz przez osobę lub organ reprezentujący podmiot kontrolowany.
2. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi.
3. W razie odmowy podpisania protokołu przez kontrolowanego administratora danych, inspektor czyni o tym wzmiankę w protokole, a odmawiający podpisu może, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi.

**Art. 17 [Upoważnienie]**
1. Jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do Generalnego Inspektora o zastosowanie środków, o których mowa w art. 18.
2. Na podstawie ustaleń kontroli inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

**Art. 18 [Naruszenie przepisów]**
1. W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje 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) wstrzymanie przekazywania danych osobowych do państwa trzeciego;
5) zabezpieczenie danych lub przekazanie ich innym podmiotom;
6) usunięcie danych osobowych.
2. Decyzje Generalnego Inspektora, o których mowa w ust. 1, nie mogą ograniczać swobody działania podmiotów zgłaszających kandydatów lub listy kandydatów w wyborach na urząd Prezydenta Rzeczypospolitej Polskiej, do Sejmu, do Senatu i do organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, pomiędzy dniem zarządzenia wyborów a dniem głosowania.
2a. Decyzje Generalnego Inspektora, o których mowa w ust. 1, w odniesieniu do zbiorów określonych w art. 43 ust. 1 pkt 1a, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa.
3. W przypadku gdy przepisy innych ustaw regulują odrębnie wykonywanie czynności, o których mowa w ust. 1, stosuje się przepisy tych ustaw.

**Art. 19 [Zawiadomienie o popełnieniu przestępstwa]** W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

**Art. 19a [Wystąpienia]**
1. W celu realizacji zadań, o których mowa w art. 12 pkt 6, Generalny Inspektor może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych.
2. Generalny Inspektor może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.
3. Podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania.

**Art. 19b [Dokonanie sprawdzenia]**
1. Generalny Inspektor może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c, o dokonanie sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia.
2. Po dokonaniu sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, administrator bezpieczeństwa informacji, za pośrednictwem administratora danych, przedstawia Generalnemu Inspektorowi sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a.
3. Dokonanie przez administratora bezpieczeństwa informacji sprawdzenia w przypadku, o którym mowa w ust. 1, nie wyłącza prawa Generalnego Inspektora do przeprowadzenia kontroli, o której mowa w art. 12 pkt 1.

**Art. 20 [Sprawozdanie]** Generalny Inspektor składa Sejmowi, raz w roku, sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych.

**Art. 21 [Wniosek o ponowne rozpatrzenie]**
1. Strona może zwrócić się do Generalnego Inspektora z wnioskiem o ponowne rozpatrzenie sprawy.
2. Na decyzję Generalnego Inspektora w przedmiocie wniosku o ponowne rozpatrzenie sprawy stronie przysługuje skarga do sądu administracyjnego.

**Art. 22 [Stosowanie KPA]** Postępowanie w sprawach uregulowanych w niniejszej ustawie prowadzi się według przepisów Kodeksu postępowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej.

**Art. 22a** *(utracił moc)*

## Rozdział 3. Zasady przetwarzania danych osobowych.

### Art. 23 [Dopuszczalność przetwarzania danych]

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. Zgoda, o której mowa w ust. 1 pkt 1, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
2a. Podmioty, o których mowa w art. 3 ust. 1, uważa się za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu.
3. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a spełnienie warunku określonego w ust. 1 pkt 1 jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.
4. Za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 5, uważa się w szczególności:
1) marketing bezpośredni własnych produktów lub usług administratora danych;
2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

### Art. 24 [Obowiązki administratora danych]

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:
1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
3) prawie dostępu do treści swoich danych oraz ich poprawiania;
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
2. Przepisu ust. 1 nie stosuje się, jeżeli:
1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;
2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

### Art. 25 [Rozszerzenie]

1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:
1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
3) źródle danych;
4) prawie dostępu do treści swoich danych oraz ich poprawiania;
5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.
2. Przepisu ust. 1 nie stosuje się, jeżeli:
1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;
2) *(uchylony)*
3) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;
4) *(uchylony)*
5) dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1, na podstawie przepisów prawa;
6) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

### Art. 26 [Nakaz zachowania szczególnej staranności]

1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
2. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:
1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych;
2) z zachowaniem przepisów art. 23 i 25.

### Art. 26a [Niedopuszczalność ostatecznych rozstrzygnięć]

1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą, albo jeżeli zezwalają na to przepisy prawa, które przewidują również środki ochrony uzasadnionych interesów osoby, której dane dotyczą.

**Art. 27 [Zakaz przetwarzania danych]**

1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:
**1)** osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
**2)** przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
**3)** przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;
**4)** jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;
**5)** przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
**6)** przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
**7)** przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
**8)** przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
**9)** jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;
**10)** przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

**Art. 28 [Numery porządkowe]**

1.*(uchylony)*
2. Numery porządkowe stosowane w ewidencji ludności mogą zawierać tylko oznaczenie płci, daty urodzenia, numer nadania oraz liczbę kontrolną.
3. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne.

**Art. 29** ***(utracił moc)***

**Art. 30** ***(utracił moc)***

**Art. 31 [Powierzenie przetwarzania danych]**

1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.
2a. Nie wymaga zawarcia umowy między administratorem a podmiotem, o którym mowa w ust. 1, powierzenie przetwarzania danych, w tym przekazywanie danych, jeżeli ma miejsce między podmiotami, o których mowa w art. 3 ust. 1.
3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.
4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.
5. Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.

**Art. 31a** ***(utracił moc)***

## Rozdział 4. Prawa osoby, której dane dotyczą.

**Art. 32 [Prawo do kontroli przetwarzania danych]**

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
**1)** uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;
7) wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;
8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;
9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a ust. 1.
2. W przypadku wniesienia żądania, o którym mowa w ust. 1 pkt 7, administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje żądanie Generalnemu Inspektorowi, który wydaje stosowną decyzję.
3. W razie wniesienia sprzeciwu, o którym mowa w ust. 1 pkt 8, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.
3a. W razie wniesienia żądania, o którym mowa w art. 32 ust. 1 pkt 9, administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi, który wydaje stosowną decyzję.
4. Jeżeli dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, administrator danych może odstąpić od informowania osób o przetwarzaniu ich danych w przypadkach, gdy pociągałoby to za sobą nakłady niewspółmierne z zamierzonym celem.
5. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1-5, nie częściej niż raz na 6 miesięcy.

**Art. 33 [Obowiązek informowania]**
1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a.
2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

**Art. 34 [Odesłanie]** Administrator danych odmawia osobie, której dane dotyczą, udzielenia informacji, o których mowa w art. 32 ust. 1 pkt 1-5a, jeżeli spowodowałoby to:
1) ujawnienie wiadomości zawierających informacje niejawne;
2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;
3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

**Art. 35 [Obowiązek uzupełnienia i sprostowania danych]**
1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.
2. W razie niedopełnienia przez administratora danych obowiązku, o którym mowa w ust. 1, osoba, której dane dotyczą, może się zwrócić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku.
3. Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

## Rozdział 5. Zabezpieczenie danych osobowych.

**Art. 36 [Środki zapewniające ochronę danych]**
1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.
3.*(uchylony)*

**Art. 36a [Administrator bezpieczeństwa informacji]**
1. Administrator danych może powołać administratora bezpieczeństwa informacji.
2. Do zadań administratora bezpieczeństwa informacji należy:
1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
3. Rejestr, o którym mowa w ust. 2 pkt 2, jest jawny. Przepis art. 42 ust. 2 stosuje się odpowiednio.
4. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w ust. 2.
5. Administratorem bezpieczeństwa informacji może być osoba, która:
1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
3) nie była karana za umyślne przestępstwo.
6. Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w ust. 5.
7. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.
8. Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań, o których mowa w ust. 2.
9. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia:
1) tryb i sposób realizacji zadań, o których mowa w ust. 2 pkt 1 lit. a i b,
2) sposób prowadzenia rejestru zbiorów danych, o którym mowa w ust. 2 pkt 2
- uwzględniając konieczność zapewnienia prawidłowości realizacji zadań administratora bezpieczeństwa informacji oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.

**Art. 36b [Niepowołanie administratora bezpieczeństwa informacji]** W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych.

**Art. 36c [Sprawozdanie]** Sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, powinno zawierać:
1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
2) imię i nazwisko administratora bezpieczeństwa informacji;
3) wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
4) datę rozpoczęcia i zakończenia sprawdzenia;
5) określenie przedmiotu i zakresu sprawdzenia;
6) opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
8) wyszczególnienie załączników stanowiących składową część sprawozdania;
9) podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej - dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania;
10) datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.

**Art. 37 [Upoważnienie do przetwarzania danych]** Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

**Art. 38 [Kontrola przetwarzania danych]** Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

**Art. 39 [Osoby zatrudnione przy przetwarzaniu danych]**
1. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
1) imię i nazwisko osoby upoważnionej;
2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
2. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

**Art. 39a [Upoważnienie dla ministra]** Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

## Rozdział 6

*(utracił moc)*

**Art. 40** ***(utracił moc)***

**Art. 41** ***(utracił moc)***

**Art. 42** ***(utracił moc)***

**Art. 43** ***(utracił moc)***

**Art. 44** ***(utracił moc)***

**Art. 44a** ***(utracił moc)***

**Art. 45** ***(utracił moc)***

**Art. 46** ***(utracił moc)***

**Art. 46a** ***(utracił moc)***

**Art. 46b** ***(utracił moc)***

**Art. 46c** ***(utracił moc)***

**Art. 46d** ***(utracił moc)***

**Art. 46e** ***(utracił moc)***

**Art. 46f** ***(utracił moc)***

## Rozdział 7. Przekazywanie danych osobowych do państwa trzeciego.

**Art. 47 [Zasady przekazywania danych]**

1. Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych.

1a. Odpowiedni poziom ochrony danych osobowych, o którym mowa w ust. 1, jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe.

2. Przepisu ust. 1 nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej, gwarantującymi odpowiedni poziom ochrony tych danych.

3. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:

1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie;

2) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie;

3) przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem;

4) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych;

5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;

6) dane są ogólnie dostępne.

**Art. 48 [Zgoda na przekazywanie danych za granicę]**

1. W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, może nastąpić po uzyskaniu zgody Generalnego Inspektora, wydanej w drodze decyzji administracyjnej, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

2. Zgoda Generalnego Inspektora nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:

1) standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 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.Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.) lub

2) prawnie wiążące reguły lub polityki ochrony danych osobowych, zwane dalej „wiążącymi regułami korporacyjnymi", które zostały zatwierdzone przez Generalnego Inspektora zgodnie z ust. 3-5.

3. Generalny Inspektor zatwierdza, w drodze decyzji administracyjnej, wiążące reguły korporacyjne przyjęte w ramach grupy przedsiębiorców do celów przekazania danych osobowych przez administratora danych lub podmiot, o którym mowa w art. 31 ust. 1, do należącego do tej samej grupy innego administratora danych lub podmiotu, o którym mowa w art. 31 ust. 1, w państwie trzecim.

4. Generalny Inspektor przed zatwierdzeniem wiążących reguł korporacyjnych może przeprowadzić konsultacje z właściwymi organami ochrony danych osobowych państw należących do Europejskiego Obszaru Gospodarczego, na których terytorium mają siedziby przedsiębiorcy należący do grupy, o której mowa w ust. 3, przekazując im niezbędne informacje w tym celu.

5. Generalny Inspektor, wydając decyzję, o której mowa w ust. 3, uwzględnia wyniki przeprowadzonych konsultacji, o których mowa w ust. 4, a jeżeli wiążące reguły korporacyjne były przedmiotem rozstrzygnięcia organu ochrony danych osobowych innego państwa należącego do Europejskiego Obszaru Gospodarczego - może uwzględnić to rozstrzygnięcie.

## Rozdział 8

*(utracił moc)*

**Art. 49** ***(utracił moc)***

**Art. 50** ***(utracił moc)***

**Art. 51** ***(utracił moc)***

**Art. 52** ***(utracił moc)***

**Art. 53** ***(utracił moc)***

**Art. 54** ***(utracił moc)***

**Art. 54a** ***(utracił moc)***

## Rozdział 9

*(utracił moc)*

**Art. 55** ***(utracił moc)***

**Art. 56** ***(utracił moc)***

**Art. 57** ***(utracił moc)***

**Art. 58** ***(utracił moc)***

**Art. 59** ***(utracił moc)***

**Art. 60** ***(utracił moc)***

**Art. 61** ***(utracił moc)***

**Art. 62** ***(utracił moc)***

1) Ustawa utraciła moc z dniem 25.05.2018 r. z wyjątkiem art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziałów 4, 5 i 7, które zachowują moc 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 27.04.2016 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).

2) Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy 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.Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.).