

Ochrona danych osobowych.

Dz.U.2016.922 t.j. z dnia 2016.06.28

Status: Akt obowiązujący

Wersja od: 1 lutego 2018 r.

Wejście w życie:

30 kwietnia 1998 r.,

13 listopada 1997 r.,

30 grudnia 1997 r.

zobacz:

art. 62

Ustawa wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia, z tym że:

- 1) art. 8-11, art. 13 i 45 wchodzi w życie po upływie 2 miesięcy od dnia ogłoszenia;
- 2) art. 55-59 wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

USTAWA

z dnia 29 sierpnia 1997 r.

o ochronie danych osobowych ¹

Rozdział 1

Przepisy ogólne

Art. 1. [Prawo do *ochrony danych osobowych*]

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. [Zakres przedmiotowy ustawy]

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 podmiotowy ustawy]

1. Ustawę stosuje się do organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych.

2. Ustawę stosuje się również do:

- 1) podmiotów niepublicznych realizujących zadania publiczne,
- 2) osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają *dane osobowe* w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych

- które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają *dane osobowe* przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Art. 3a. [Wyłączenia z zakresu stosowania ustawy]

1. Ustawy nie stosuje się do:

- 1) osób fizycznych, które przetwarzają *dane* wyłącznie w celach osobistych lub domowych;
- 2) podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania *danych*.

2. Ustawy, z wyjątkiem przepisów art. 14-19 i art. 36 ust. 1, nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. poz. 24, z późn. zm.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której *dane* dotyczą.

Art. 4. [Pierwszeństwo umów międzynarodowych]

Przepisów ustawy nie stosuje się, jeżeli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej.

Art. 5. [Zbieg przepisów]

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. [Definicja *danych osobowych*]

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 ustawowy]

Ilekoć 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 jakiegokolwiek 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. [Generalny Inspektor Ochrony Danych Osobowych]

1. Organem do spraw *ochrony danych osobowych* jest Generalny Inspektor *Ochrony Danych Osobowych*, zwany dalej "Generalnym Inspektorem".

2. Generalnego Inspektora powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu.

3. Na stanowisko Generalnego Inspektora może być powołany ten, kto łącznie spełnia następujące warunki:

- 1) jest obywatelem polskim i stale zamieszkuje na terytorium Rzeczypospolitej Polskiej;
- 2) wyróżnia się wysokim autorytetem moralnym;
- 3) posiada wyższe wykształcenie prawnicze oraz odpowiednie doświadczenie zawodowe;
- 4) nie był karany za przestępstwo.

4. Generalny Inspektor w zakresie wykonywania swoich zadań podlega tylko ustawie.

5. Kadencja Generalnego Inspektora trwa 4 lata, licząc od dnia złożenia ślubowania. Po upływie kadencji Generalny Inspektor pełni swoje obowiązki do czasu objęcia stanowiska przez nowego Generalnego Inspektora.
6. Ta sama osoba nie może być Generalnym Inspektorem więcej niż przez dwie kadencje.
7. Kadencja Generalnego Inspektora wygasa z chwilą jego śmierci, odwołania lub utraty obywatelstwa polskiego.
8. Sejm, za zgodą Senatu, odwołuje Generalnego Inspektora, jeżeli:
 - 1) zrzekł się stanowiska;
 - 2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby;
 - 3) sprzeniewierzył się złożonemu ślubowaniu;
 - 4) został skazany prawomocnym wyrokiem sądu za popełnienie przestępstwa.

Art. 9. [Ślubowanie]

Przed przystąpieniem do wykonywania obowiązków Generalny Inspektor składa przed Sejmem następujące ślubowanie:

"Obejmując stanowisko Generalnego Inspektora *Ochrony Danych Osobowych* uroczyście ślubuję dochować wierności postanowieniom Konstytucji Rzeczypospolitej Polskiej, strzec prawa do *ochrony danych osobowych*, a powierzone mi obowiązki wypełniać sumiennie i bezstronnie."

Ślubowanie może być złożone z dodaniem słów "Tak mi dopomóż Bóg".

Art. 10. [Zakaz zajmowania innych stanowisk]

1. Generalny Inspektor nie może zajmować innego stanowiska, z wyjątkiem stanowiska profesora szkoły wyższej, ani wykonywać innych zajęć zawodowych.
2. Generalny Inspektor nie może należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.

Art. 11. [Immunitet]

1. Generalny Inspektor nie może być bez uprzedniej zgody Sejmu pociągnięty do odpowiedzialności karnej ani pozbawiony wolności, z zastrzeżeniem ust. 2.
2. Generalny Inspektor może wyrazić zgodę na pociągnięcie go do odpowiedzialności karnej za wykroczenia, o których mowa w ust. 3, w trybie określonym w tym przepisie.
3. W przypadku popełnienia przez Generalnego Inspektora wykroczenia, o którym mowa w rozdziale XI ustawy z dnia 20 maja 1971 r. - Kodeks wykroczeń (Dz. U. z 2015 r. poz. 1094, 1485, 1634 i 1707), przyjęcie przez Generalnego Inspektora mandatu karnego albo uiszczenie grzywny, w przypadku ukarania mandatem karnym zaocznym, o którym mowa w art. 98 § 1 pkt 3 ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2013 r. poz. 395, z późn. zm.), stanowi oświadczenie o wyrażeniu przez niego zgody na pociągnięcie go do odpowiedzialności w tej formie.
4. Generalny Inspektor nie może być zatrzymany lub aresztowany, z wyjątkiem ujęcia go na gorącym uczynku przestępstwa i jeżeli jego zatrzymanie jest niezbędne do zapewnienia prawidłowego toku postępowania. O zatrzymaniu niezwłocznie powiadamia się Marszałka Sejmu, który może nakazać natychmiastowe zwolnienie zatrzymanego.

Art. 11a. [Przedawnienie czynu objętego immunitetem]

Przedawnienie w postępowaniu karnym czynu objętego immunitetem nie biegnie w okresie

korzystania z immunitetu.

Art. 11b. [Wniosek o wyrażenie zgody na pociągnięcie Generalnego Inspektora do odpowiedzialności karnej]

1. Wniosek o wyrażenie zgody na pociągnięcie Generalnego Inspektora do odpowiedzialności karnej w sprawie o przestępstwo ścigane z oskarżenia publicznego składa się za pośrednictwem Prokuratora Generalnego.
2. Wniosek o wyrażenie zgody na pociągnięcie Generalnego Inspektora do odpowiedzialności karnej w sprawie o przestępstwo ścigane z oskarżenia prywatnego składa oskarżyciel prywatny, po wniesieniu sprawy do sądu.
3. Wniosek, o którym mowa w ust. 2, sporządza i podpisuje adwokat lub radca prawny, z wyjątkiem wniosków składanych w swoich sprawach przez sędziów, prokuratorów, adwokatów, radców prawnych, notariuszy oraz profesorów i doktorów habilitowanych nauk prawnych.
4. Wnioski, o których mowa w ust. 1 i 2, powinny zawierać:
 - 1) oznaczenie wnioskodawcy oraz pełnomocnika, o ile został ustanowiony;
 - 2) imię i nazwisko oraz datę i miejsce urodzenia Generalnego Inspektora;
 - 3) wskazanie podstawy prawnej wniosku;
 - 4) dokładne określenie czynu, którego dotyczy wniosek, ze wskazaniem czasu, miejsca, sposobu i okoliczności jego popełnienia oraz jego skutków, a zwłaszcza charakteru powstałej szkody;
 - 5) uzasadnienie.

Art. 11c. [Rozpatrzenie wniosku o wyrażenie zgody na pociągnięcie Generalnego Inspektora do odpowiedzialności karnej]

1. Wniosek o wyrażenie zgody na pociągnięcie Generalnego Inspektora do odpowiedzialności karnej składa się Marszałkowi Sejmu.
2. Jeżeli wniosek nie spełnia wymogów formalnych, o których mowa w art. 11b ust. 3 lub 4, Marszałek Sejmu wzywa wnioskodawcę do poprawienia lub uzupełnienia wniosku w terminie 14 dni, wskazując niezbędny zakres poprawienia lub uzupełnienia. W przypadku niepoprawienia lub nieuzupełnienia wniosku we wskazanym terminie i zakresie Marszałek Sejmu postanawia o pozostawieniu wniosku bez biegu.
3. Jeżeli wniosek spełnia wymogi formalne, o których mowa w art. 11b ust. 3 i 4, Marszałek Sejmu kieruje go do organu właściwego na podstawie regulaminu Sejmu do rozpatrzenia wniosku, zawiadamiając jednocześnie Generalnego Inspektora o treści wniosku.
4. Organ właściwy do rozpatrzenia wniosku powiadamia Generalnego Inspektora o terminie rozpatrzenia wniosku. Pomiędzy doręczeniem powiadomienia a terminem rozpatrzenia wniosku, o ile nie zachodzi wypadek niecierpiący zwłoki, powinno upłynąć co najmniej 7 dni.
5. Na żądanie organu właściwego do rozpatrzenia wniosku sąd albo odpowiedni organ, przed którym toczy się postępowanie wobec Generalnego Inspektora, udostępnia akta postępowania.
6. Generalny Inspektor przedstawia organowi właściwemu do rozpatrzenia wniosku wyjaśnienia i własne wnioski w tej sprawie w formie pisemnej lub ustnej.

7. Po rozpatrzeniu sprawy, organ właściwy do rozpatrzenia wniosku uchwala sprawozdanie wraz z propozycją przyjęcia lub odrzucenia wniosku.
 8. W trakcie rozpatrywania przez Sejm sprawozdania, o którym mowa w ust. 7, Generalnemu Inspektorowi przysługuje prawo do zabrania głosu.
 9. Sejm wyraża zgodę na pociągnięcie Generalnego Inspektora do odpowiedzialności karnej w drodze uchwały podjętej bezwzględną większością ustawowej liczby posłów.
- Nieuzyskanie wymaganej większości głosów oznacza podjęcie uchwały o niewyrażeniu zgody na pociągnięcie Generalnego Inspektora do odpowiedzialności karnej.

Art. 11d. [Wyrażenie zgody na zatrzymanie lub aresztowanie Generalnego Inspektora]

1. Zakaz zatrzymania, o którym mowa w art. 11, obejmuje wszelkie formy pozbawienia lub ograniczenia wolności osobistej Generalnego Inspektora przez organy stosujące przymus.
2. Wniosek o wyrażenie zgody na zatrzymanie lub aresztowanie Generalnego Inspektora składa się za pośrednictwem Prokuratora Generalnego.
3. Wniosek, o którym mowa w ust. 2, powinien zawierać:
 - 1) oznaczenie wnioskodawcy;
 - 2) imię i nazwisko oraz datę i miejsce urodzenia Generalnego Inspektora;
 - 3) dokładne określenie czynu oraz jego kwalifikację prawną;
 - 4) podstawę prawną zastosowania określonego środka;
 - 5) uzasadnienie, wskazujące w szczególności na konieczność zastosowania określonego środka.
4. Do postępowania z wnioskiem o wyrażenie zgody na zatrzymanie lub aresztowanie Generalnego Inspektora przepisy art. 11c ust. 1-8 stosuje się odpowiednio.
5. Sejm wyraża zgodę na zatrzymanie lub aresztowanie Generalnego Inspektora w drodze uchwały podjętej bezwzględną większością ustawowej liczby posłów. Nieuzyskanie wymaganej większości głosów oznacza podjęcie uchwały o niewyrażeniu zgody na zatrzymanie lub aresztowanie Generalnego Inspektora.
6. Wymóg uzyskania zgody Sejmu nie dotyczy wykonania kary pozbawienia wolności orzeczonej prawomocnym wyrokiem sądu.

Art. 11e. [Ogłoszenie uchwał o wyrażeniu zgody na pociągnięcie do odpowiedzialności karnej lub na zatrzymanie albo aresztowanie]

1. Marszałek Sejmu przesyła wnioskodawcy niezwłocznie uchwałę, o której mowa w art. 11c ust. 9 i art. 11d ust. 5.
2. Uchwały, o których mowa w ust. 1, podlegają ogłoszeniu w Dzienniku Urzędowym Rzeczypospolitej Polskiej "Monitor Polski".

Art. 11f. [Przepisy stosowane do odpowiedzialności za wykroczenia]

Przepisy ustawy dotyczące odpowiedzialności karnej Generalnego Inspektora stosuje się odpowiednio do odpowiedzialności za wykroczenia.

Art. 11g. [Stosowanie przepisów regulaminu Sejmu]

Szczegółowy tryb postępowania w sprawach, o których mowa w art. 11a-11f, określa regulamin Sejmu.

Art. 12. [Zadania Generalnego Inspektora *Ochrony Danych Osobowych*]

Do zadań Generalnego Inspektora w szczególności należy:

- 1) kontrola zgodności przetwarzania *danych* z przepisami o *ochronie danych osobowych*;
- 2) wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o *ochronie danych osobowych*;
- 3) zapewnienie wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji, o których mowa w pkt 2, przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2016 r. poz. 599);
- 4) prowadzenie rejestru zbiorów *danych* oraz rejestru administratorów bezpieczeństwa informacji, a także udzielanie informacji o zarejestrowanych zbiorach *danych* i zarejestrowanych administratorach bezpieczeństwa informacji;
- 5) opiniowanie projektów ustaw i rozporządzeń dotyczących *ochrony danych osobowych*;
- 6) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia *ochrony danych osobowych*;
- 7) uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką *ochrony danych osobowych*.

Art. 12a. [Zastępca Generalnego Inspektora *Ochrony Danych Osobowych*]

1. Na wniosek Generalnego Inspektora Marszałek Sejmu może powołać zastępcę Generalnego Inspektora. Odwołanie zastępcy Generalnego Inspektora następuje w tym samym trybie.

2. Generalny Inspektor określa zakres zadań swojego zastępcy.

3. Zastępca Generalnego Inspektora powinien spełniać wymogi określone w art. 8 ust. 3 pkt 1, 2 i 4 oraz posiadać wyższe wykształcenie i odpowiednie doświadczenie zawodowe.

Art. 13. [Biuro Generalnego Inspektora *Ochrony Danych Osobowych*]

1. Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora *Ochrony Danych Osobowych*, zwanego dalej Biurem.

1a. Generalny Inspektor w przypadkach uzasadnionych charakterem i liczbą spraw z zakresu *ochrony danych osobowych* na *danym* terenie może wykonywać swoje zadania przy pomocy jednostek zamiejscowych Biura.

2. (uchylony).

3. Prezydent Rzeczypospolitej Polskiej, po zasięgnięciu opinii Generalnego Inspektora, w drodze rozporządzenia, nadaje statut Biuru, określając jego organizację, zasady działania oraz siedziby jednostek zamiejscowych i zakres ich właściwości terytorialnej, mając na uwadze stworzenie optymalnych warunków organizacyjnych do prawidłowej realizacji zadań Biura.

Art. 14. [Kompetencje Generalnego Inspektora *Ochrony Danych Osobowych* i 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 6⁰⁰ do 22⁰⁰, 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. [Uprawnienia kontrolne]

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. [Środki stosowane po kontroli]

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 o *ochronie danych osobowych*]

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 i wnioski Generalnego Inspektora *Ochrony Danych Osobowych*]

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 wnioski, 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. [Wniosek o dokonanie sprawdzenia zgodności przetwarzania *danych osobowych* z przepisami o *ochronie danych osobowych*]

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. [Roczne sprawozdanie z działalności]

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 sprawy]

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 przepisów k.p.a.]

Postępowanie w sprawach uregulowanych w niniejszej ustawie prowadzi się według przepisów Kodeksu postępowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej.

Art. 22a. [Delegacja ustawowa - wzory upoważnień i legitymacji służbowych]

Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wzór upoważnienia i legitymacji służbowej, o których mowa w art. 14 pkt 1, uwzględniając konieczność imiennego wskazania inspektora Biura Generalnego Inspektora *Ochrony Danych Osobowych*.

Rozdział 3

Zasady przetwarzania *danych osobowych*

Art. 23. [Przesłanki dopuszczalności przetwarzania *danych osobowych*]

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. [Informacje przekazywane osobie, której dane są zbierane]

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. [Zbieranie danych osobowych nie od osoby, której one dotyczą]

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. [Główne obowiązki administratora danych]

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. [Zakaz podejmowania decyzji w sprawach indywidualnych wyłącznie na podstawie automatycznego przetwarzania *danych osobowych*]

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 wnioski osoby, której *dane* dotyczą, albo jeżeli zezwalają na to przepisy prawa, które przewidują również środki *ochrony* uzasadnionych interesów osoby, której *dane* dotyczą.

Art. 27. [*Dane wrażliwe*]

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 stosowane w ewidencji ludności]

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.

(uchylony).

Art. 30.

(uchylony).

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

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. [Przetwarzanie *danych* przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim]

W przypadku przetwarzania *danych osobowych* przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim, administrator *danych* jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej.

Rozdział 4

Prawa osoby, której *dane* dotyczą

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

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. [Informowanie osób o przysługujących im prawach]

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. [Odmowa udzielenia informacji]

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 poprawienia lub usunięcia *danych osobowych*]

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. [Obowiązek zabezpieczenia *danych osobowych*]

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, zabranieniem 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 o zgodności przetwarzania *danych osobowych* z przepisami o ochronie *danych osobowych*]

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. [Osoby uprawnione do przetwarzania *danych*]

Do przetwarzania *danych* mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora *danych*.

Art. 38. [Kontrola wprowadzania i przekazywania *danych osobowych*]

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. [Ewidencja osób upoważnionych do przetwarzania *danych osobowych*]

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. [Delegacja ustawowa - sposób prowadzenia dokumentacji, wymogi w odniesieniu do urządzeń i systemów informatycznych]

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

Rejestracja zbiorów *danych osobowych* oraz administratorów bezpieczeństwa informacji

Art. 40. [Zgłoszenie zbioru *danych* do rejestracji]

Administrator *danych* jest obowiązany zgłosić zbiór *danych* do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a.

Art. 41. [Treść zgłoszenia zbioru *danych*]

1. Zgłoszenie zbioru *danych* do rejestracji powinno zawierać:

- 1) wniosek o wpisanie zbioru do rejestru zbiorów *danych osobowych*;
- 2) oznaczenie administratora *danych* i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia przetwarzania *danych* podmiotowi, o którym mowa w art. 31, lub wyznaczenia podmiotu, o którym mowa w art. 31a, oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania;
- 3) cel przetwarzania *danych*;
- 3a) opis kategorii osób, których *dane* dotyczą, oraz zakres przetwarzanych *danych*;
- 4) sposób zbierania oraz udostępniania *danych*;
- 4a) informację o odbiorcach lub kategoriach odbiorców, którym *dane* mogą być przekazywane;
- 5) opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39;
- 6) informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a;

7) informację dotyczącą ewentualnego przekazywania *danych* do państwa trzeciego.

2. Administrator *danych* jest obowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania zmiany w zbiorze *danych*, z zastrzeżeniem ust. 3.

3. Jeżeli zmiana informacji, o której mowa w ust. 1 pkt 3a, dotyczy rozszerzenia zakresu przetwarzanych *danych* o *dane*, o których mowa w art. 27 ust. 1, administrator *danych* jest obowiązany do jej zgłoszenia przed dokonaniem zmiany w zbiorze.

4. Do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów *danych*.

Art. 42. [Rejestr zbiorów *danych* osobowych]

1. Generalny Inspektor prowadzi ogólnokrajowy, jawny rejestr zbiorów *danych* osobowych. Rejestr powinien zawierać informacje, o których mowa w art. 41 ust. 1 pkt 1-4a i 7.

2. Każdy ma prawo przeglądać rejestr, o którym mowa w ust. 1.

3. Na żądanie administratora *danych* może być wydane zaświadczenie o zarejestrowaniu zgłoszonego przez niego zbioru *danych*, z zastrzeżeniem ust. 4.

4. Generalny Inspektor wydaje administratorowi *danych*, o których mowa w art. 27 ust. 1, zaświadczenie o zarejestrowaniu zbioru *danych* niezwłocznie po dokonaniu rejestracji.

Art. 43. [Zwolnienie z obowiązku rejestracji zbioru *danych*]

1. Z obowiązku rejestracji zbioru *danych* zwolnieni są administratorzy *danych*:

1) zawierających informacje niejawne;

1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności;

2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym;

2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej;

2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;

2c) przetwarzanych przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej;

3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego;

4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się;

5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta;

6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego;

- 7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności;
- 8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
- 9) powszechnie dostępnych;
- 10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego;
- 11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego;
- 12) przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających *dane*, o których mowa w art. 27 ust. 1.

1a. Obowiązkowi rejestracji zbiorów *danych osobowych*, z wyjątkiem zbiorów zawierających *dane*, o których mowa w art. 27 ust. 1, nie podlega administrator *danych*, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi do rejestracji, z zastrzeżeniem art. 46e ust. 2.

2. ² W odniesieniu do zbiorów, o których mowa w ust. 1 pkt 1 i 3, oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego, Służbę Ochrony Państwa oraz Centralne Biuro Antykorupcyjne, Generalnemu Inspektorowi nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1 i 3-5 oraz art. 15-18.

Art. 44. [Odmowa rejestracji zbioru *danych*]

1. Generalny Inspektor wydaje decyzję o odmowie rejestracji zbioru *danych*, jeżeli:

- 1) nie zostały spełnione wymogi określone w art. 41 ust. 1;
- 2) przetwarzanie *danych* naruszałoby zasady określone w art. 23-28;
- 3) urządzenia i systemy informatyczne służące do przetwarzania zbioru *danych* zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a.

2. Odmawiając rejestracji zbioru *danych*, Generalny Inspektor, w drodze decyzji administracyjnej, nakazuje:

- 1) ograniczenie przetwarzania wszystkich albo niektórych kategorii *danych* wyłącznie do ich przechowywania lub
- 2) zastosowanie innych środków, o których mowa w art. 18 ust. 1.

3. (uchylony).

4. Administrator *danych* może zgłosić ponownie zbiór *danych* do rejestracji po usunięciu wad, które były powodem odmowy rejestracji zbioru.

5. W razie ponownego zgłoszenia zbioru do rejestracji administrator *danych* może rozpocząć ich przetwarzanie po zarejestrowaniu zbioru.

Art. 44a. [Wykreślenie z rejestru zbioru *danych osobowych*]

Wykreślenie z rejestru zbiorów *danych osobowych* jest dokonywane, w drodze decyzji administracyjnej, jeżeli:

- 1) zaprzestano przetwarzania *danych* w zarejestrowanym zbiorze;
- 2) rejestracji dokonano z naruszeniem prawa.

Art. 45.

(uchylony).

Art. 46. [Rozpoczęcie przetwarzania *danych* w zbiorze *danych*]

1. Administrator *danych* może, z zastrzeżeniem ust. 2, rozpocząć ich przetwarzanie w zbiorze *danych* po zgłoszeniu tego zbioru Generalnemu Inspektorowi, chyba że ustawa zwalnia go z tego obowiązku.
2. Administrator *danych*, o których mowa w art. 27 ust. 1, może rozpocząć ich przetwarzanie w zbiorze *danych* po zarejestrowaniu zbioru, chyba że ustawa zwalnia go z obowiązku zgłoszenia zbioru do rejestracji.

Art. 46a. [Delegacja ustawowa - wzór zgłoszenia zbioru *danych*]

Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wzór zgłoszenia, o którym mowa w art. 41 ust. 1, uwzględniając obowiązek zamieszczenia informacji niezbędnych do stwierdzenia zgodności przetwarzania *danych* z wymogami ustawy.

Art. 46b. [Zgłoszenie powołania i odwołania administratora bezpieczeństwa informacji]

1. Administrator *danych* jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.
2. Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:
 - 1) oznaczenie administratora *danych* i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;
 - 2) *dane* administratora bezpieczeństwa informacji:
 - a) imię i nazwisko,
 - b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość,
 - c) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 1;
 - 3) datę powołania;
 - 4) oświadczenie administratora *danych* o spełnianiu przez administratora bezpieczeństwa informacji warunków określonych w art. 36a ust. 5 i 7.
3. Zgłoszenie odwołania administratora bezpieczeństwa informacji powinno zawierać:
 - 1) *dane*, o których mowa w ust. 2 pkt 1 i pkt 2 lit. a i b;
 - 2) datę i przyczynę odwołania.
4. Na żądanie administratora *danych* lub administratora bezpieczeństwa informacji Generalny Inspektor wydaje zaświadczenie o zarejestrowaniu administratora bezpieczeństwa informacji.
5. Administrator *danych* jest obowiązany zgłosić Generalnemu Inspektorowi zmianę informacji objętych zgłoszeniem, o którym mowa w ust. 2, w terminie 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania administratora bezpieczeństwa informacji.

Art. 46c. [Rejestr administratorów bezpieczeństwa informacji]

Generalny Inspektor prowadzi ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji, zawierający informacje, o których mowa w art. 46b ust. 2 pkt 1 i pkt 2 lit. a i c.

Art. 46d. [Wykreślenie administratora bezpieczeństwa informacji z rejestru]

1. Wykreślenie administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji następuje po powiadomieniu o jego odwołaniu albo w przypadku jego śmierci.

2. Generalny Inspektor z urzędu wydaje administratorowi *danych* decyzję o wykreśleniu administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji, jeżeli:

- 1) administrator bezpieczeństwa informacji nie spełnia warunków określonych w art. 36a ust. 5 lub 7;
- 2) administrator bezpieczeństwa informacji nie wykonuje zadań określonych w art. 36a ust. 2;
- 3) administrator *danych* nie powiadomił o odwołaniu administratora bezpieczeństwa informacji.

3. Do administratora *danych* będącego adresatem decyzji, o której mowa w ust. 2, nie stosuje się zwolnienia, o którym mowa w art. 43 ust. 1a.

Art. 46e. [Ponowne zgłoszenie powołania administratora bezpieczeństwa informacji]

1. W przypadku ponownego zgłoszenia przez administratora *danych* do rejestracji Generalnemu Inspektorowi powołania administratora bezpieczeństwa informacji wykreślonego z rejestru administratorów bezpieczeństwa informacji na podstawie art. 46d ust. 2, Generalny Inspektor, w drodze decyzji administracyjnej:

- 1) wpisuje administratora bezpieczeństwa informacji do rejestru administratorów bezpieczeństwa informacji po stwierdzeniu, że nie zachodzą przyczyny wykreślenia z rejestru, o których mowa w art. 46d ust. 2 pkt 1 i 2;
- 2) odmawia wpisania administratora bezpieczeństwa informacji do rejestru administratorów bezpieczeństwa informacji, jeżeli nie zostały usunięte przyczyny wykreślenia z rejestru, o których mowa w art. 46d ust. 2 pkt 1 i 2.

2. Do administratora *danych*, który ponownie zgłosił do rejestracji administratora bezpieczeństwa informacji wykreślonego na podstawie art. 46d ust. 2, zwolnienie z obowiązku rejestracji zbioru określone w art. 43 ust. 1a stosuje się po wpisaniu zgłoszonego administratora bezpieczeństwa informacji do rejestru administratorów bezpieczeństwa informacji.

Art. 46f. [Delegacja ustawowa - wzór zgłoszenia administratora bezpieczeństwa informacji]

Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wzory zgłoszeń administratora bezpieczeństwa informacji, o których mowa w art. 46b ust. 2 i 3, uwzględniając konieczność zapewnienia Generalnemu Inspektorowi informacji niezbędnych do prawidłowego realizowania jego zadań.

Przekazywanie *danych osobowych* do państwa trzeciego

Art. 47. [Warunki przekazania *danych osobowych* do państwa trzeciego]

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 Generalnego Inspektora *Ochrony Danych Osobowych* na przekazanie *danych osobowych* do państwa trzeciego]

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

"wiązącymi 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

Przepisy karne

Art. 49. [Niedopuszczalne przetwarzanie *danych osobowych*]

1. Kto przetwarza w zbiorze *dane osobowe*, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli czyn określony w ust. 1 dotyczy *danych* ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, *danych* o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 50.

(uchylony).

Art. 51. [Udostępnianie *danych osobowych* osobom nieupoważnionym]

1. Kto administrując zbiorem *danych* lub będąc obowiązany do *ochrony danych osobowych* udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 52. [Naruszenie obowiązku zabezpieczenia *danych osobowych*]

Kto administrując *danymi* narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53. [Nie zgłoszenie zbioru *danych* do rejestracji]

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru *danych*, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54. [Niepoinformowanie o prawach osoby, której dane są przetwarzane]

Kto administrując zbiorem *danych* nie dopełnia obowiązku poinformowania osoby, której *dane* dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54a. [Utrudnianie wykonywania czynności kontrolnych]

Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Rozdział 9

Zmiany w przepisach obowiązujących, przepisy przejściowe i końcowe

Art. 55.

W ustawie z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 20, poz. 101, z 1982 r. Nr 31, poz. 214, z 1985 r. Nr 22, poz. 98 i Nr 50, poz. 262, z 1987 r. Nr 21, poz. 123, z 1989 r. Nr 34, poz. 178, z 1991 r. Nr 100, poz. 443, z 1993 r. Nr 1, poz. 1, z 1995 r. Nr 34, poz. 163 i Nr 142, poz. 701, z 1996 r. Nr 73, poz. 350, Nr 89, poz. 402, Nr 106, poz. 496 i Nr 139, poz. 647 oraz z 1997 r. Nr 75, poz. 469) w art. 2 w pkt 2 po wyrazach "Rzecznika Praw Obywatelskich," dodaje się wyrazy "Generalnego Inspektora *Ochrony Danych Osobowych*,".

Art. 56.

W ustawie z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. Nr 31, poz. 214, z 1984 r. Nr 35, poz. 187, z 1988 r. Nr 19, poz. 132, z 1989 r. Nr 4, poz. 24, Nr 34, poz. 178 i 182, z 1990 r. Nr 20, poz. 121, z 1991 r. Nr 55, poz. 234, Nr 88, poz. 400 i Nr 95, poz. 425, z 1992 r. Nr 54, poz. 254 i Nr 90, poz. 451, z 1994 r. Nr 136, poz. 704, z 1995 r. Nr 132, poz. 640, z 1996 r. Nr 89, poz. 402 i Nr 106, poz. 496 oraz z 1997 r. Nr 98, poz. 604) wprowadza się następujące zmiany: (zmiany pominięte).

Art. 57.

W ustawie z dnia 5 stycznia 1991 r. - Prawo budżetowe (Dz. U. z 1993 r. Nr 72, poz. 344, z 1994 r. Nr 76, poz. 344, Nr 121, poz. 591 i Nr 133, poz. 685, z 1995 r. Nr 78, poz. 390, Nr 124, poz. 601 i Nr 132, poz. 640, z 1996 r. Nr 89, poz. 402, Nr 106, poz. 496, Nr 132, poz. 621 i Nr 139, poz. 647 oraz z 1997 r. Nr 54, poz. 348, Nr 79, poz. 484, Nr 121, poz. 770 i Nr 123, poz. 775 i 778) w art. 31 w ust. 3 w pkt 2 po wyrazach "Najwyższej Izby Kontroli" dodaje się wyrazy ", Generalnego Inspektora *Ochrony Danych Osobowych*".

Art. 58.

W ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59, z 1996 r. Nr 64, poz. 315 i Nr 89, poz. 402 oraz z 1997 r. Nr 28, poz. 153, Nr 79, poz. 484, Nr 96, poz. 589 i Nr 121, poz. 770) w art. 4 wprowadza się następujące zmiany: (zmiany pominięte).

Art. 59.

W ustawie z dnia 23 grudnia 1994 r. o kształtowaniu środków na wynagrodzenia w

państwowej sferze budżetowej oraz o zmianie niektórych ustaw (Dz. U. z 1995 r. Nr 34, poz. 163 oraz z 1996 r. Nr 106, poz. 496 i Nr 139, poz. 647) w art. 2 w ust. 2 w pkt 1 po wyrazach "Krajowym Biurze Wyborczym" dodaje się wyrazy ", Biurze Generalnego Inspektora Ochrony Danych Osobowych."

Art. 60.

W ustawie z dnia 26 kwietnia 1996 r. o Służbie Więziennej (Dz. U. Nr 61, poz. 283 i Nr 106, poz. 496 oraz z 1997 r. Nr 28, poz. 153 i Nr 88, poz. 554) dodaje się art. 23a w brzmieniu: (zmiany pominięte).

Art. 61. [Zarejestrowanie zbiorów *danych* prowadzonych przed wejściem w życie ustawy]

1. Podmioty określone w art. 3, prowadzące w dniu wejścia w życie ustawy zbiory *danych osobowych* w systemach informatycznych, mają obowiązek złożenia wniosków o zarejestrowanie tych zbiorów w trybie określonym w art. 41, w terminie 18 miesięcy od dnia jej wejścia w życie, chyba że ustawa zwalnia ich z tego obowiązku.

2. Do czasu rejestracji zbioru *danych osobowych* w trybie określonym w art. 41, podmioty, o których mowa w ust. 1, mogą prowadzić te zbiory bez rejestracji.

Art. 62. [Wejście w życie ustawy]

Ustawa wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia, z tym że:

- 1) art. 8-11, art. 13 i 45 wchodzi w życie po upływie 2 miesięcy od dnia ogłoszenia;
- 2) art. 55-59 wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

¹ 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.).

² Art. 43 ust. 2 zmieniony przez art. 282 ustawy z dnia 8 grudnia 2017 r. (Dz.U.2018.138) zmieniającej nin. ustawę z dniem 1 lutego 2018 r.