Administracja bezpieczeństwa, informacji niejawnych i danych osobowych

Seria wydawnicza Wydziału Nauk o Bezpieczeństwie

Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego

„BEZPIECZEŃSTWO I OBRONNOŚĆ”

5

Administracja bezpieczeństwa, informacji niejawnych i danych osobowych

Vademecum

Zbiór i opracowanie:
Jerzy Depo, Sławomir Mazur

Krakowska Akademia
im. Andrzeja Frycza Modrzewskiego
Wydział Nauk o Bezpieczeństwie

2015 bezpieczeństwo i obronność

Redakcja naukowa: Mieczysław Bieniek, Sławomir M. Mazur

Recenzent: prof. dr hab. inż. Piotr Sienkiewicz

Publikacja powstała w ramach projektu badawczego Krakowskiej Akademii
im. Andrzeja Frycza Modrzewskiego
nr WNoB/DS/1/2014/KON

Projekt okładki: Oleg Aleksejczuk

Na okładce rewers medalu „Memoria Gratum Facit – Za zasługi dla Wydziału Nauk
o Bezpieczeństwie Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego"
autorstwa Czesława Dźwigaja

ISBN 978-83-65208-30-9

Na zlecenie:
Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego

www.ka.edu.pl

Wydawca: Oficyna Wydawnicza AFM KAAFM, Kraków 2015

Sprzedaż prowadzi: Księgarnia U Frycza
tel./faks: (12) 252 45 93; e-mail: ksiegarnia@kte.pl

Skład: Oleg Aleksejczuk

Druk i oprawa: MKpromo

Spis treści

Wykaz skrótów

ABI	administrator bezpieczeństwa informacji
ABW	Agencja Bezpieczeństwa Wewnętrznego
art.	artykuł
AW	Agencja Wywiadu
BND	Bundesnachrichtendienst
BOR	Biuro Ochrony Rządu
CIA	Central Intelligence Agency
CBA	Centralne Biuro Antykorupcyjne
CBŚ	Centralne Biuro Śledcze
DEA	Drug Enforcement Administration
Dz.U.	Dziennik Ustaw
FBI	Federal Bureau of Investigation
GIIF	Generalny Inspektor Informacji Finansowej
GIODO	Generalny Inspektor Ochrony Danych Osobowych
kk	Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 z późn. zm.)
Konstytucja RP	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze sprost. i z późn. zm.)
KWS	Konwencja wykonawcza do Układu z Schengen z dnia 14 czerwca 1985 r. między rządami państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach.
NBP	Narodowy Bank Polski
NIK	Najwyższa Izba Kontroli
PBE	procedury bezpiecznej eksploatacji
PBI	polityka bezpieczeństwa informacji
pp	Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24 z późn. zm.)
SC	Służba Celna
SIS	System Informacyjny Schengen (Schengen Information System)
SG	Straż Graniczna

SKW	Służba Kontrwywiadu Wojskowego
SW	Służba Więzienna
SWB	szczególne wymagania bezpieczeństwa
SWW	Służba Wywiadu Wojskowego
SZBI	system zarządzania bezpieczeństwem informacji
uodo	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r. Nr 133, poz. 883 z późn. zm.)
uoin	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228 z późn. zm.)
UOP	Urząd Ochrony Państwa
UdSC	Urząd do Spraw Cudzoziemców
ust.	ustęp
VIS	Wizowy System Informacyjny (Visa Information System)
ŻW	Żandarmeria Wojskowa

By zachować posiadaną tajemnicę,
nie wystarczy samo milczenie.
Paul Claudel (1868–1955)

Wprowadzenie

Bezpieczeństwo informacyjne jest jednym z priorytetowych elementów bezpieczeństwa państwa, a także podstawą sprawnego funkcjonowania różnych innych jednostek organizacyjnych.

Dziś obrona bezpieczeństwa informacyjnego, gdy rywalizacja między przeciwnikami politycznymi, biznesowymi, wojskowymi i innymi, przeniosła się na płaszczyznę walki informacyjnej i jest ukierunkowana nie tylko na zdobywanie informacji przeróżnymi metodami i technikami, ale i na sterowanie procesami decyzyjnymi przeciwnika (blokowanie przepływu informacji, szerzenie dezinformacji, sianie niepokoju oraz podważanie autorytetu i zaufania do zaatakowanego podmiotu), jest zadaniem szczególnym.

Potrzeba dysponowania skutecznymi środkami polityki bezpieczeństwa informacyjnego jest zatem duża, a dbałość o bezpieczne warunki egzystencji państwa (bronienie dostępu do własnych tajemnic) winna się wiązać nierozerwalnie z potrzebą ciągłego rozpoznawania otoczenia (konkurencji i potencjalnego przeciwnika).

W pracy, która ma być pomocą dydaktyczną dla studentów wszystkich kierunków studiów, na których poruszane są podstawowe wiadomości z dziedziny bezpieczeństwa, zaprezentowano organizacyjno-prawne podejście do problemu ochrony informacji niejawnych i danych osobowych. Zamieszczone w niej definicje, reguły i praktyczne wskazówki mają bowiem na celu przybliżenie i usystematyzowanie terminologii stosowanej w tej dziedzinie wiedzy i działalności. Ponadto z uwagi na interdyscyplinarny charakter poruszanych zagadnień niniejsza praca kierowana jest też do szerszego grona odbiorców, przede wszystkim do kierowników jednostek organizacyjnych, którzy w świetle prawa są odpowiedzialni za informacje prawnie chronione, gromadzone zgodnie z prawem przetwarzania danych osobowych obywateli.

Poszczególne rozdziały opracowania zostały zgrupowane w trzech częściach tematycznych: część pierwsza – *Ochrona informacji niejawnych*, część druga – *Ochrona danych osobowych*, i część trzecia – *Systemy informacyjne Schengen (SIS i VIS) a ochrona informacji niejawnych i danych osobowych.* Każdą część zamyka oddzielny zestaw bibliografii, a do części pierwszej i trzeciej w formie aneksów załączono wybrane akty prawne.

Część pierwsza
Ochrona informacji niejawnych

1. Ochrona informacji niejawnych w polskim systemie prawnym

Jednym z obszarów aktywności państwa w dziedzinie bezpieczeństwa zewnętrznego i wewnętrznego oraz jego obywateli jest regulacja spraw związanych z ochroną informacji niejawnych. Na przestrzeni wieków podejmowano ją w różnych aspektach i różnych formach, a przede wszystkim w reakcji na uprawiane od ponad 5 tys. lat szpiegostwo. Posiadanie, dostęp i technologie rozpowszechniania informacji są bowiem ważnym czynnikiem bezpieczeństwa i rozwoju państwa. Dlatego dziś, gdy rozwój cywilizacji i techniki przekazu implikuje nowe zagrożenia (przestępstwa komputerowe, cyberterroryzm), zagadnienie to jest szczególnie ważne.

Ochrona aktywów informacyjnych w systemie bezpieczeństwa państwa polskiego nie jest niczym nowym. Zasadnicze działania związane z prawnymi i technicznymi jej aspektami były i są podejmowane na szczeblu najwyższych władz państwowych. Idea społeczeństwa informacyjnego obejmuje już praktycznie wszystkie sfery działalności organów administracji państwowej, samorządowej i przedsiębiorstw gospodarczych. Tematyka zagrożeń i bezpieczeństwo informacji stanowi również przedmiot licznych studiów i prac naukowych.

W pierwszym dziesięcioleciu niepodległej Polski (1918–1927) ustawodawstwo dotyczące ochrony informacji oparto na zmodyfikowanych przepisach prawa karnego byłych państw zaborczych – Rosji z 1903 r., Niemiec z 1871 r. i Austrii z 1852 r.[1]

W Drugiej Rzeczypospolitej o obowiązku ochrony tajemnicy stanowiły:

- Rozporządzenie Prezydenta RP z 16 lutego 1928 r. – Kary za szpiegostwo i niektóre inne przestępstwa przeciwko Państwu (Dz.U. z 1928 r. Nr 18, poz. 160)[2];

---

[1] Więcej informacji na temat historii ochrony informacji niejawnych w Polsce – zob. S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010, s. 9–25; *Idem*, *Karnoprawna ochrona informacji*, Opole 2009, s. 13–27; S. Hoc, J. Zaleśny, *Ochrona informacji niejawnych w Rzeczypospolitej Polskiej*, [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009, s. 261–281.

[2] Uchylono w 1934 r. nowym rozporządzeniem.

- Ustawa z dnia 17 lutego 1922 r. o państwowej służbie cywilnej (Dz.U. z 1922 r. Nr 21, poz. 164);
- Rozporządzenie Prezydenta RP z dnia 11 lipca 1932 r. – Kodeks karny (Dz.U. z 1932 r. Nr 60, poz. 571);
- Rozporządzenie Prezydenta RP z dnia 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu Państwa (Dz.U. z 1934 r. Nr 94, poz. 851);
- Dekret Prezydenta RP z dnia 22 listopada 1938 r. o ochronie niektórych interesów Państwa (Dz.U. z 1938 r. Nr 91, poz. 623).

Po drugiej wojnie światowej system ochrony tajemnicy kształtowały:

- Dekret z 13 czerwca 1946 r. o przestępstwach szczególnie niebezpiecznych w okresie odbudowy państwa (Dz.U. z 1946 r. Nr 30, poz. 192)[3];
- Dekret z 26 października 1949 r. o ochronie tajemnicy państwowej i służbowej (Dz.U. z 1949 r. Nr 55, poz. 437 ze zm.)[4];
- Uchwała nr 282/59 Rady Ministrów w sprawie organizacji ochrony tajemnicy państwowej i służbowej;
- Zarządzenie nr 70/60 Ministra Spraw Wewnętrznych z dnia 31 marca 1960 r. w sprawie postępowania w kraju z dokumentami tajnymi i tajnymi specjalnego znaczenia wraz z załącznikiem w postaci Instrukcji Ministra Spraw Wewnętrznych wydanej w porozumieniu z Ministrem Obrony Narodowej o postępowaniu w kraju z dokumentami tajnymi, tajnymi specjalnego znaczenia oraz dokumentami geodezyjnymi, kartograficznymi i geologicznymi stanowiącymi tajemnicę państwową i służbową;
- Ustawa z dnia 19 kwietnia 1969 r. – Kodeks karny wykonawczy (Dz.U. z 1969 r. Nr 13, poz. 98);
- Uchwała nr 126/71 Rady Ministrów z dnia 2 lipca 1971 r. w sprawie organizacji ochrony tajemnicy państwowej i służbowej;
- Zarządzenie nr 89/72 Ministra Spraw Wewnętrznych z dnia 30 sierpnia 1972 r. w sprawie zasad i sposobu postępowania w kraju z wiadomościami stanowiącymi tajemnicę państwową i służbową wraz z załącznikiem w postaci instrukcji wzorcowej;
- Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej (Dz.U. z 1982 r. Nr 40, poz. 271)[5].

---

[3] Uchylony 1 stycznia 1970 r.

[4] Uchylono na mocy art. 6 pkt 9 Ustawy z dnia 19 kwietnia 1969 r. – Przepisy wprowadzające Kodeks karny (Dz.U. z 1969 r. Nr 13, poz. 95).

[5] Ustawa ta obowiązywała prawie do końca lat 90. XX w. W sposób szczególny ochronę tajemnicy regulowała w epoce Polski Ludowej Konstytucja Polskiej Rzeczypospolitej Ludowej z dnia 22 lipca 1952 r. (Dz.U. z 1952 r. Nr 33, poz. 232), która w art. 79 zawierała zapis: „1. Czujność wobec wrogów narodu oraz pilne strzeżenie tajemnicy państwowej jest obowiązkiem każdego obywatela Polskiej Rzeczypospolitej Ludowej. 2. Zdrada Ojczyzny: szpiegostwo, osłabienie sił zbrojnych, przejście na stronę wroga karane jest z całą surowością prawa jako najwyższa zbrodnia".

W okresie przemian ustrojowych, ubiegania się Polski o przyjęcie do struktur euro-atlantyckich, w pierwszych latach członkostwa w NATO i UE oraz dostosowywania polskiego prawa do rozwiązań w tych organizacjach, podstawą prawa ochrony informacji niejawnych w Polsce była Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2005 r. Nr 196, poz. 1631 ze zm.).

Aktualnie głównymi aktami prawnymi określającymi zasady i organizację systemu ochrony informacji niejawnych w RP są:

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze sprost. i późn. zm.);
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228 z późn. zm.);
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r. Nr 133, poz. 883 z późn. zm.[6]);
- Ustawa z dnia 4 lutego 1999 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.);
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r. Nr 112, poz. 1198 z późn. zm.);
- ratyfikowane bilateralne umowy międzynarodowe (porozumienia, memoranda) o wzajemnej ochronie informacji niejawnych oraz inne polskie ustawy i akty wykonawcze odnoszące się do tego obszaru, a w szczególności:
- Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2000 r. Nr 98, poz. 1071 z późn. zm.);
- Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. z 1964 r. Nr 43, poz. 296 z późn. zm.);
- Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (t.j. Dz.U. z 2015 r. poz. 827 z późn. zm.);
- Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (t.j. Dz.U. z 2014 r. poz. 1502 z późn. zm.);
- Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych (t.j. Dz.U. z 2013 r. poz. 269 z późn. zm.);
- Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz.U. z 2011 r. Nr 123, poz. 698 późn. zm.);
- Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24 z późn. zm.);
- Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2007 r. Nr 43, poz. 277 z późn. zm.);
- Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz.U z 2014 r. poz. 1402 z późn. zm.);

---

[6] Na chwilę obecną obowiązuje jednolity tekst ustawy o ochronie danych osobowych dostosowany do wymogów zamieszczonych w Obwieszczeniu Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 25 listopada 2015 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych (Dz.U. z 2015 r. poz. 2135) t.j. tekst opracowany na podstawie Dz.U. z 2015 r. poz. 2135, 2281, Dz.U. z 2016 r. poz. 195.

- Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2003 r. Nr 153, poz. 1503 z późn. zm.);
- Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (t.j. z 2014 r. poz. 1099 z późn. zm.);
- Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (t.j. Dz.U. z 2007 r. Nr 231, poz. 1701 z późn. zm.);
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 z późn. zm.);
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 1997 r. Nr 89, poz. 555 z późn. zm.);
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz.U. z 1997 r. Nr 90, poz. 557 z późn. zm.);
- Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym (t.j. Dz.U. z 2007 r. Nr 36, poz. 232 z późn. zm.);
- Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2005 r. Nr 145, poz. 1221 z późn. zm.);
- Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz.U. z 2015 r. poz. 128 z późn. zm.);
- Ustawa z dnia 18 grudnia 1998 o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (t.j. Dz.U z 2007 r. Nr 63, poz. 424 z późn. zm.);
- Ustawa z dnia 16 marca 2001 r. o Biurze Ochrony Rządu (t.j. Dz.U. z 2004 r. Nr 163, poz. 1712 z późn. zm.);
- Ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (t.j. Dz.U. z 2010 r. Nr 29, poz. 153);
- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U z 2001 r. Nr 128, poz. 1402 z późn. zm.);
- Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (t.j. Dz.U. z 2013 r. poz. 395 z późn. zm.);
- Ustawa z dnia 24 sierpnia 2001 o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2001 r. Nr 123, poz.1353 z późn. zm.);
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2014 r. poz. 782 z późn. zm.);
- Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2010 r. Nr 29, poz. 154);
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2013 r. poz. 1422);
- Ustawa z dnia 12 czerwca 2003 r. – Prawo pocztowe (t.j. Dz.U. z 2008 r. Nr 189, poz. 1159 z późn. zm.);
- Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz.U. z 2010 r. Nr 95, poz. 593 z późn. zm.);
- Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2014 r. poz. 243 z późn. zm.);
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2014 r. poz. 1114 z późn. zm.);

- Ustawa z dnia 8 lipca 2005 r. o Prokuratorii Generalnej Skarbu Państwa (Dz.U. z 2005 r. Nr 169, poz. 1914 z późn. zm.);
- Ustawa z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j. Dz.U. z 2014 r. poz. 1411 z późn. zm.);
- Ustawa z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2006 r. Nr 104, poz. 709 z późn. zm.);
- Ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (t.j. Dz.U. z 2014 r. poz. 253 z późn. zm.);
- Ustawa z dnia 18 października 2006 r. o ujawnieniu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów (t.j. Dz.U. z 2007 r. Nr 63, poz. 425 z późn. zm.);
- Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz.U. z 2008 r. Nr 199, poz. 1227 z późn. zm.);
- Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej (t.j. Dz.U. z 2014 r. poz. 990 z późn. zm.);
- Ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz.U. z 2010 r. Nr 81, poz. 530 z późn. zm.);

a także rozporządzenia i inne przepisy resortowe niezbędne do stosowania przepisów przedmiotowych ustaw, m.in.:

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024);
- Rozporządzenie Prezesa Rady Ministrów z 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz.U. z 2010 r. Nr 258, poz. 1750);
- Rozporządzenie Prezesa Rady Ministrów z 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz.U. z 2010 r. Nr 258, poz. 1751);
- Rozporządzenie Prezesa Rady Ministrów z 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U. z 2010 r. Nr 258, poz. 1752);
- Rozporządzenie Prezesa Rady Ministrów z 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U. z 2010 r. Nr 258, poz. 1753);
- Rozporządzenie Prezesa Rady Ministrów z 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U. z 2010 r. Nr 258, poz. 1754);

- Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. Nr 14, poz. 67 z późn. zm.);
- Rozporządzenie Rady Ministrów z dnia 5 kwietnia 2011 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz.U. z 2011 r. Nr 86, poz. 470);
- Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz.U. z 2011 r. Nr 93, poz. 541);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz.U. z 2011 r. Nr 156, poz. 926);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r. Nr 159, poz. 948);
- Rozporządzenie Prezesa Rady Ministrów z dnia 4 października 2011 r. w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa (Dz.U. z 2011 r. Nr 220, poz. 1302);
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. z 2011 r. Nr 271, poz. 1603);
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2011 r. Nr 276, poz. 1631);
- Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. z 2011 r. Nr 288, poz. 1692);
- Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r. poz. 683);
- Wytyczne Agencji Bezpieczeństwa Wewnętrznego Krajowej Władzy Bezpieczeństwa z dnia 31 grudnia 2010 r. w sprawie postępowania z informacjami niejawnymi międzynarodowymi;
- Decyzja Nr 165/MON Ministra Obrony Narodowej z dnia 29 kwietnia 2011 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (Dz.Urz.MON z 2011 r. poz. 127);
- Decyzja Nr 17/MON Ministra Obrony Narodowej z 20 stycznia 2012 r. w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej (Dz.Urz. MON z 2012 r. poz. 8);

- Decyzja Nr 61/MON Ministra Obrony Narodowej z dnia 5 marca 2012 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej (Dz.Urz.MON z 2012 r. poz. 86);
- Zarządzenie Nr 45 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 17 sierpnia 2012 r. w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych.

Ponadto w związku z przystąpieniem do NATO i UE Polska została zobligowana do ratyfikowania i respektowania wielu umów międzysojuszniczych, z których kluczowymi są:

- Umowa między Stronami Traktatu Północnoatlantyckiego w sprawie ochrony informacji, sporządzona w Brukseli dnia 6 marca 1997 r. (Dz.U. z 2000 r. Nr 64, poz. 740);
- Umowa organizacji Traktatu Północnoatlantyckiego o przekazywaniu informacji technicznych dla celów obronnych, sporządzona w Brukseli 19 października 1970 r. (Dz.U. z 2000 r. Nr 64, poz. 742);
- Umowa o wzajemnej ochronie tajemnicy wynalazków dotyczących obronności, w przypadku których zostały złożone wnioski o udzielenie patentów, sporządzona w Paryżu 21 września 1960 r. (Dz.U. z 2000 r. Nr 64, poz. 744);
- Umowa między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych, sporządzona w Paryżu dnia 18 czerwca 1964 r. (Dz.U. z 2001 r. Nr 143, poz. 1594);
- Traktat między Królestwem Belgii […] a […] Rzecząpospolitą Polską […] dotyczący przystąpienia […] Rzeczypospolitej Polski […] do Unii Europejskiej [tzw. Traktat Akcesyjny], podpisany w Atenach dnia 16 kwietnia 2003 r. (Dz.U. z 2004 r. Nr 90, poz. 864 z późn. zm.).

2. Podstawowe pojęcia i zakres stosowania uregulowań ustawowych

Jednym z podstawowych standardów demokratycznego państwa prawa jest zagwarantowanie wszystkim jego obywatelom jednakowych wolności, praw i obowiązków, w tym prawa do szeroko rozumianej autonomii informacyjnej.

W Konstytucji RP z dnia 2 kwietnia 1997 r. do katalogu wolności i praw w tej dziedzinie należą:

- wolność prasy i innych środków społecznego przekazu (art. 14 Konstytucji);
- prawo do prawnej ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (art. 47 Konstytucji);
- wolność i ochrona tajemnicy komunikowania się (art. 49 Konstytucji);
- prawo ochrony danych osobowych (art. 51 Konstytucji);
- wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji, gwarantowana zakazem cenzury prewencyjnej i koncesjonowania prasy (art. 54 Konstytucji);

- prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne (art. 61 Konstytucji);
- prawo do informacji o stanie i ochronie środowiska (art. 74 ust. 3 Konstytucji).

Zgodnie z art. 31 ust. 3 Konstytucji ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawianie „tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności praw innych osób”[7]. W każdym jednak razie ograniczenia – nawet te wprowadzane w drodze ustawowej – nie mogą naruszać istoty tych praw i wolności.

Aktem prawnym ingerującym w sferę pewnych swobód obywatelskich jest m.in. przedmiotowa ustawa o ochronie informacji niejawnych. Szczególnego rodzaju przesłankami przyjęcia przez ustawodawcę zawartych w niej ograniczeń dostępu do informacji – przez objęcie określonych informacji klauzulami tajności oraz ustanowienie procedur i rygorów postępowania są:

- troska o dobro wspólne (art. 1 Konstytucji – „Rzeczpospolita jest dobrem wspólnym wszystkich obywateli”);
- strzeżenie niepodległości i nienaruszalności terytorium RP (art. 5 Konstytucji);
- ochrona informacji, których ujawnienie mogłoby spowodować szkody dla RP albo byłoby z punktu widzenia jej interesów niekorzystne (zbiór wartości chronionych w obszarze bezpieczeństwa wewnętrznego i porządku konstytucyjnego[8]).

Zgodnie z art. 1 ust. 2 pkt 1–6 uoin przepisy ustawy, a także wydane do niej przepisy wykonawcze, mają zastosowanie do:

a) organów władzy publicznej (Sejmu i Senatu, prezydenta RP, organów administracji rządowej, organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych, sądów i trybunałów, organów kontroli państwowej i ochrony prawa);
b) jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych;
c) NBP;
d) państwowych osób prawnych i innych niż wymienione w pkt 1–3 państwowych jednostek organizacyjnych;
e) jednostek organizacyjnych podległych organom władzy publicznej lub przez nie nadzorowanych;
f) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

---

[7] Szerzej zob. L. Garlicki, *Komentarz do art. 31 Konstytucji RP*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 3, red. L. Garlicki, Warszawa 2003, s. 23–28.

[8] M. Jabłoński, T. Radziszewski, *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, Wrocław 2012, s. 19–27.

Z kolei zgodnie z art. 3 ust. 1 i 2 uodo jej postanowienia mają zastosowanie do:

a) organów państwowych (organów władzy państwowej: Sejmu, Senatu, prezydenta RP oraz organów administracji rządowej);
b) organów samorządu terytorialnego;
c) innych państwowych i komunalnych jednostek organizacyjnych;
d) podmiotów niepublicznych realizujących zadania publiczne;
e) osób fizycznych i osób prawnych;
f) jednostek organizacyjnych nie mających osobowości prawnej, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub czynią to dla realizacji celów statutowych.

Wymienione podmioty są zobowiązane stosować regulacje Ustawy o ochronie danych osobowych, jeżeli mają siedzibę albo miejsce zamieszkania na terytorium RP, albo w państwie trzecim, jeżeli przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium RP (art. 3 ust. 2 uodo).

Ustawę stosuje się do przetwarzania danych osobowych (art. 2 ust. 2 uodo):

a) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych;
b) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych[9].

Ustawa nie ma zaś zastosowania (art. 3a uodo) do:

a) osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych;
b) podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim i wykorzystujących środki techniczne znajdujące się na terytorium RP wyłącznie do przekazywania danych;
c) do prasowej działalności dziennikarskiej[10], literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą;
d) jeżeli umowa międzynarodowa, której stroną jest RP, stanowi inaczej (art. 4 uodo).

Zgodnie z definicjami zawartymi w przepisach ogólnych przedmiotowych ustaw, a także w rozumieniu delegacji w podanych wyżej zarządzeniach wykonawczych:

1. Akredytacją bezpieczeństwa teleinformatycznego jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych (art. 2 pkt 10 uoin).

---

9 „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 poddawanych anonimizacji, mają zastosowanie wyłącznie zasady ich zabezpieczenia" (art. 2 ust. 3 uodo).

10 W rozumieniu Prawa prasowego.

2. Aktywa informacyjne to informacja, nośniki używane do jej przechowywania i dystrybucji, usługi, oprogramowanie i sprzęt.

3. Ankieta bezpieczeństwa osobowego jest jednym z elementów postępowania sprawdzającego, dokumentem wypełnianym przez osobę sprawdzaną, który ma umożliwić organowi przeprowadzającemu postępowanie ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Ankieta powinna zostać wypełniona przez osobę sprawdzaną własnoręcznie i zgodnie z jej najlepszą wiedzą i wolą. Formularz ankiety składa się z siedmiu części:

- część I – Dane osobowe – zawiera podstawowe dane o osobie;
- część II – Dane osobowe członków oraz współmieszkańców osoby sprawdzanej;
- część III – Dane dotyczące historii życia zawodowego i osobistego – zawierające dane (dotyczące okresu po ukończeniu 18 roku życia) odnośnie do:
  - historii zatrudnienia,
  - dostępu do informacji niejawnych,
  - ostatniej ukończonej szkoły, wszystkich szkół ukończonych po 18 roku życia, a także kursów zagranicznych i posiadanego wykształcenia oraz tytułów naukowych,
  - członkostwa w partiach politycznych, stowarzyszeniach, organizacjach społecznych oraz we władzach fundacji, adresów zamieszkania dłuższych niż 30 dni;
- część IV – Dane dotyczące bezpieczeństwa – zawierają pytania o:
  - współpracę lub pracę w organach bezpieczeństwa PRL,
  - karalność za przestępstwa,
  - toczące się aktualnie postępowania karne,
  - toczące się aktualnie postępowania dyscyplinarne związane z naruszeniem przepisów dotyczących ochrony informacji niejawnych,
  - zainteresowanie ze strony obcych służb specjalnych i/lub grup przestępczych (także wobec członków rodziny i/lub współmieszkańców),
  - wypytywanie przez obce władze na tematy związane z bezpieczeństwem i obronnością RP (także wobec członków rodziny i/lub współmieszkańców),
  - pobyty zagraniczne (także partnera) dłuższe niż 30 dni,
  - kontakty (także partnera) z obywatelami innych państw;
- część V – Dane dotyczące stanu zdrowia – zawierają pytania o:
  - kategorię zdrowia (stwierdzoną w wyniku badania np. w wojsku),
  - przebyte lub aktualne choroby psychiczne,
  - przebyte lub aktualne dolegliwości psychiczne,
  - zażywanie środków odurzających i psychotropowych,
  - spożywanie alkoholu w ilościach powodujących utratę świadomości,
  - problemy w pracy lub życiu prywatnym spowodowane spożywaniem alkoholu,
  - leczenie się w związku ze spożywaniem alkoholu;
- część VI – Dane dotyczące sytuacji majątkowo-finansowej – zawierają pytania dotyczące:

- wynagrodzenia,
- innych dochodów,
- łącznych dochodów za poprzedni rok,
- składania oświadczeń o stanie majątkowym,
- osób prowadzących wspólne gospodarstwo domowe z osobą sprawdzaną (w tym numery PESEL i NIP tych osób oraz zestawienia ich rocznych dochodów),
- liczby osób na utrzymaniu osoby sprawdzanej,
- posiadanych nieruchomości (także innych osób ze wspólnego gospodarstwa domowego),
- posiadanych firm lub udziałów w firmie,
- posiadanych ruchomości, których koszt nabycia był wyższy niż 20 tys. zł,
- posiadanych rachunków bankowych,
- zadłużenia i innych zobowiązań finansowych;

- część VII – Osoby polecające (co najmniej trzy).

W przypadku postępowań zwykłych nie wypełnia się części V–VI, a część VII wypełniają tylko osoby ubiegające się o dostęp do informacji niejawnych o klauzuli „ściśle tajne".

Po wypełnieniu ankieta bezpieczeństwa osobowego stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „poufne" w przypadku poszerzonego postępowania sprawdzającego lub „zastrzeżone" w przypadku zwykłego postępowania sprawdzającego (art. 24 ust. 10 uoin). Ankiecie ani formalnie, ani technicznie nie nadaje się klauzuli tajności, ale w rozumieniu ustawy staje się ona po wypełnieniu dokumentem niejawnym przez 20 lat jej przechowywania.

4. Atrybuty (domeny, przedmioty) bezpieczeństwa informacji niejawnych[11]:

- poufność – zapewnienie, że dostęp do danej informacji mają wyłącznie osoby uprawnione;
- integralność danych – zapewnienie, że informacje niejawne są przechowywane w oryginalnej postaci, tzn. że nie zostały zmodyfikowane (zniekształcone lub zmienione) w sposób nieuprawniony;
- integralność systemu – zapewnienie, że system realizuje swoje funkcje w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, przypadkowej lub zamierzonej;
- dostępność – zapewnienie, że zasób danego systemu jest możliwy do wykorzystania na żądanie, w określonym czasie i tylko przez podmiot uprawniony;
- autentyczność – oznacza możliwość jednoznacznego stwierdzenia, jaki podmiot przesłał dane;
- rozliczalność – dotyczy możliwości identyfikacji użytkowników informacji i systemu teleinformatycznego oraz wykonywanych przez nich usług,

[11] Literatura przedmiotu przedstawia trzy podstawowe sytuacje, w których ma być chroniona informacja: 1) dostęp do informacji, 2) transmisja informacji, 3) przechowywanie informacji. Dlatego, bezpieczeństwo informacji przejawia się w jej ochronie przed: a) zniszczeniem, b) nieuprawnionym ujawnieniem, c) modyfikacją; por. *Zarządzanie bezpieczeństwem informacyjnym*, red. A. Nowak, W. Scheffs, Warszawa 2020, s. 46.

- niezaprzeczalność – ochrona przed fałszywym zaprzeczeniem przez nadawcę faktu wysłania danych, a przez odbiorcę – faktu otrzymania danych[12].

5. Audyt systemu ochrony informacji niejawnych – to specjalistyczna forma oceny, czy wprowadzone i realizowane działania są zgodne z przyjętą polityką i opracowanymi procedurami bezpieczeństwa i czy skutecznie chronią jej aktywa. Analizie w trakcie audytu powinny zostać poddane: lokalizacja obiektu, systemy zabezpieczeń, zabezpieczenia budowlane, zabezpieczenia mechaniczne, zabezpieczenia techniczne, systemy alarmowe (sygnalizacji napadu i włamania), systemy kontroli dostępu, systemy wykrywania pożaru i ochrona fizyczna. Audyt przeprowadzony zgodnie ze ściśle określoną metodologią[13] umożliwia:

- sprawdzenie aktualnego stanu bezpieczeństwa informacji, wskazanie konkretnych nieprawidłowości i niezgodności;
- sprecyzowanie wytycznych techniczno-organizacyjnych do opracowania prawidłowo funkcjonującego systemu bezpieczeństwa informacji;
- opracowanie wytycznych do rozwiązań w zakresie prawidłowego funkcjonowania systemu bezpieczeństwa informacji w danej jednostce organizacyjnej;
- opracowanie wytycznych dotyczących prawidłowej organizacji ochrony technicznej, fizycznej i monitoringu;
- opracowanie innych niezbędnych wytycznych wynikających ze specyfiki funkcjonującego systemu bezpieczeństwa informacji[14].

---

[12] Za: M. Pańkowska, *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2004.

[13] Za szczególny wzór służą w tym względzie normy ISO – Międzynarodowej Organizacji Normalizacyjnej (International Organization for Standardization), wywodzące się z brytyjskiego standardu BS 7799-2, które w każdej edycji są poszerzane o nowe elementy i stanowią najszerzej stosowany zestaw wskazówek do wdrożenia i utrzymania systemu bezpieczeństwa informacji. Stosuje się je zarówno do informacji papierowej, jak i informacji przechowywanej w systemach informatycznych, a zakres ich stosowania może obejmować całość informacji przetwarzanej w danej instytucji, albo tylko jeden wydzielony system (np. system oddziału, departamentu itp.). Poza zdefiniowaniem ogólnego modelu zarządzania bezpieczeństwem informacji normy ISO definiują również poszczególne elementy kontroli i sterowania bezpieczeństwem informacji, podporządkowując je odpowiednim zakresom wymagań. ISO nie jest skrótem, lecz oficjalną nazwą przyjętą przez państwa członkowskie tej międzynarodowej organizacji, wśród których znajduje się Polski Komitet Normalizacyjny. ISO ustanawia normy we wszystkich dziedzinach naszego życia. Od chwili powstania w 1947 r. do 2009 r. ISO ustanowiła i wprowadziła ponad 17 tys. norm. Np. norma ustanawiająca bezpieczeństwo informacji nosi nazwę ISO 27001 – Technika informatyczna – Technika bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania (ramka). Polskie normy wywodzące się z norm ISO mają zapis: np. norma: Systemy zarządzania bezpieczeństwem informacji. Wymagania – PN-ISO/IEC 27005:2007, norma: Praktyczne zasady zarządzania bezpieczeństwem informacji – PN ISO/IEC 17799:2005, a norma: Zarządzanie ryzykiem – Zasady i wytyczne – PN-ISO 31000:2012.

[14] Ustawa o ochronie informacji niejawnych mówi zaledwie w kilku przypadkach o audycie systemu ochrony informacji niejawnych w jednostce organizacyjnej i nazywa go bardzo różnie, w zależności od tego, czego dany audyt ma dotyczyć, mówi więc o kontroli, sprawdzeniu lub akredytacji. Np. w art. 10 uoin przyznaje ABW i SKW upraw-

6. Bezpieczeństwo fizyczne informacji niejawnych – to system powiązanych ze sobą przedsięwzięć organizacyjnych, osobowych, technicznych i fizycznych służących ochronie tych informacji przed nieuprawnionym dostępem, ingerencją w ich treść, uszkodzeniem lub utratą[15].

7. Bezpieczeństwo informacyjne – to zespół działań, metod, struktur organizacyjnych i procedur podejmowanych przez uprawnione podmioty dla ochrony systemów, sieci i zasobów informacyjnych przed ich niepożądanym lub nieuprawnionym ujawnieniem[16], modyfikacją bądź zniszczeniem[17]. Bezpieczeństwo informacji można osiągnąć, wdrażając odpowiedni zestaw zabezpieczeń. Przy czym celowe jest, aby te zabezpieczenia były ustanawiane, wdrażane i mo-

---

nienia do kontroli ochrony informacji niejawnych i jest to pierwszy zapis w ustawie, który uprawnia te podmioty do przeprowadzenia w jednostce organizacyjnej audytu systemu ochrony informacji niejawnych. Następny zapis uprawniający przedstawicieli ABW i SKW do przeprowadzenia audytu systemu ochrony informacji niejawnych został umieszczony w art. 48 ust. 1 uoin. Zgodnie z tym przepisem systemy i sieci teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego. Zaś w art. 57 uoin mówi się o sprawdzeniu w toku postępowania bezpieczeństwa przemysłowego systemu ochrony osób, materiałów i obiektów u przedsiębiorcy.

15 Zob. cyt. norma PN-ISO/IEC 17799. Przystępując do budowy systemu ochrony zasobów informacyjnych (informatycznych), należy odpowiedzieć sobie na pytania: co chronimy?, przed czym chronimy i w jaki sposób chronimy? Głównymi elementami bezpieczeństwa fizycznego są: a) działania prewencyjne – opracowanie planów, instrukcji, regulaminów i procedur ochrony, b) ochrona aktywna (czynna) – zorganizowanie własnej wewnętrznej służby ochrony (dozorcy, portierzy, recepcjoniści, wartownicy, patrole interwencyjne) lub korzystanie z usług koncesjonowanych agencji ochrony (SUFO – specjalizowane uzbrojone formacje ochronne), c) ochrona bierna – wydzielenie, zorganizowanie i wdrożenie zabezpieczeń architektoniczno-budowlanych (ogrodzenie, bramy, zapory, przegrody, ściany, stropy, drzwi, okna, szyby, zamki, kłódki, kraty, sejfy, szafy metalowe, szafy ognioodporne itp.), d) elektroniczne zabezpieczenie i kontrola wejść i wyjść, e) zastosowanie zabezpieczeń mechanicznych w postaci tripodów, śluz, bramek magnetycznych itp.

16 Ujawnienie jest pojęciem szerokim. Obejmuje to, co nazywamy wyjawieniem tajemnicy, udzieleniem komuś wiadomości stanowiących tajemnicę, zakomunikowaniem, rozpowszechnieniem bądź opublikowaniem. Forma czy sposób ujawnienia mogą być różne – może to być wypowiedź ustna, udostępnienie pisma zawierającego informacje niejawne, okazanie dokumentu lub przedmiotu, opublikowanie w masowych środkach przekazu, przekazanie informacji niejawnej za pomocą technicznych środków przekazu, np. telefonu czy faksu. Formą ujawnienia może być również znak lub sygnał. Ujawnienie jest bezprawne, jeśli informacja posiadająca atrybut poufności zostanie przekazana poza krąg osób prawnie do niej dopuszczonych lub wówczas, gdy zostanie pozbawiona tego atrybutu wbrew obowiązkowi dyskrecji. I. Stankowska, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2011, s. 15.

17 Por. P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2005, s. 71; *Zarządzanie bezpieczeństwem informacyjnym*…, s. 24. Definicję pojęcia bezpieczeństwa informacyjnego możemy także znaleźć w normach ISO (zob. przypis 17): norma PN-ISO/IEC 27001:2007 oraz norma PN-ISO/IEC 17799:2007.

nitorowane, przeglądane i w razie potrzeby ulepszane oraz powiązane z innymi procesami zarządzania funkcjonującymi w organizacji.

8. Bezpieczeństwo teleinformatyczne – to zakres przedsięwzięć mających na celu uniemożliwienie niepowołanym osobom dostępu do systemów i sieci teleinformatycznych (TI)[18].

9. Certyfikat – dokument potwierdzający pozytywną ocenę bezpieczeństwa środków, urządzeń lub narzędzi przeznaczonych do ochrony informacji niejawnych (art. 2 pkt 11 uoin)[19].

10. Informacja – potocznie definiowana jest w powiązaniu z przedmiotami myślowymi, które odzwierciedlają różnorodne postacie wiadomości, wieści czy też wiedzy o aktualnych zdarzeniach[20]. W *Encyklopedii popularnej PWN* pojęcie to interpretowane jest jako czynnik[21], dzięki któremu człowiek lub urządzenie automatycznie mogą przeprowadzić bardziej sprawne, celowe działanie (informacja sterująca), a w *Słowniku współczesnym języka polskiego* informacja to

---

[18] Bezpieczeństwo teleinformatyczne obejmuje ochronę fizyczną, ochronę elektromagnetyczną, ochronę kryptograficzną, ochronę transmisji oraz kontrolę dostępu do systemu i sieci teleinformatycznych. Na podstawie art. 62 ust. 1 uoin zostało wydane Rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. W § 1 tego aktu określono główne wymagania bezpieczeństwa teleinformatycznego, jakim winny odpowiadać systemy i sieci teleinformatyczne służące do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, oraz sposób opracowywania dokumentów SWB i PBE systemów lub sieci teleinformatycznych. Zgodnie z § 3 przedmiotowego rozporządzenia bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności. Dlatego też zadaniem kierownika danej komórki organizacyjnej, na którym *de facto* bezpośrednio spoczywa obowiązek ochrony informacji niejawnych oraz właściwej organizacji bezpieczeństwa teleinformatycznego, powinno być przede wszystkim zastosowaniem takich procedur oraz środków ochrony fizycznej informacji, które zminimalizują możliwość utraty wewnętrznych atrybutów bezpieczeństwa.

[19] Zgodnie z art. 46 pkt 4 uoin jednostki organizacyjne dysponujące informacjami niejawnymi o klauzuli „poufne" lub wyższej są zobligowane do stosowania wyposażenia i urządzeń służących do przechowywania lub ochrony materiałów niejawnych (szaf metalowych, systemów dozorowych, alarmowych itp.), a także systemów teleinformatycznych służących do przetwarzania informacji niejawnych, którym na podstawie odrębnych przepisów przyznano certyfikaty. Certyfikację wyrobów służących ochronie informacji niejawnych przeprowadzają jednostki posiadające akredytację Polskiego Centrum Akredytacji. Urządzenia wyprodukowane, zakupione i zamontowane w okresie ważności certyfikatu zachowują ważność przez cały okres eksploatacji. Urządzenie traci jednak certyfikat w przypadku dokonania zmian konstrukcyjnych lub w przypadku zmiany przepisów. Wyroby, na które wydano certyfikat zgodności, podlegają oznakowaniu potwierdzającemu zgodność wyrobu z zasadniczymi wymaganiami.

[20] W. Kopaliński, *Słownik wyrazów obcych*, Warszawa 1980, s. 429.

[21] *Encyklopedia popularna PWN*, red. A. Karwowski, Warszawa 1982, s. 294.

„element wiedzy przekazywanej za pomocą języka lub innego kodu i stanowi czynnik zmniejszający stopień niewiedzy o jakimś zjawisku, umożliwiający człowiekowi polepszenie znajomości otoczenia i sprawniejsze przeprowadzenie celowego działania”[22]. Natomiast w literaturze prawniczej informację definiuje się jako „wiadomość lub sumę wiadomości o sytuacjach, stanach rzeczy, wydarzeniach i osobach”[23].

11. Informacje międzynarodowe niejawne – to informacje pochodzące od podmiotów zagranicznych lub wytworzone w ich interesie, wymagające ochrony przed nieuprawnionym dostępem lub ujawnieniem na poziomie wskazanym przez odwołanie się do klauzul tajności obowiązujących w RP (art. 5 ust. 5 uoin)[24].

12. Informacje niejawne – to informacje, „których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania” (art. 1 ust. 1 uoin)[25].

---

[22] *Słownik współczesny języka polskiego*, red. B. Dunaj, Warszawa 1998, s. 320.

[23] Niejednokrotnie w codziennym życiu pojęcie „informacja” stosujemy zamiennie, używając określeń „wiadomości” lub „dane”. Mimo iż nie są to synonimy, generalnie nie popełniamy błędu. Pamiętać jednak należy, że określenia „dane” używa się najczęściej do oznaczania informacji nieprzetworzonej i są nimi np. niezbite liczby i fakty odzwierciedlające pojedynczy aspekt otaczającej nas rzeczywistości. Natomiast wiadomość to doniesienie o czymś nowym, czego brak w dotychczasowym stanie świadomości odbiorcy.

[24] Informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznacza się polskim odpowiednikiem posiadanej klauzuli tajności; w języku angielskim są to: 1) dla NATO: *cosmic top secret* – „ściśle tajne”, *NATO secret* – „tajne”, *NATO confidential* – „poufne”, *NATO restricted* – „zastrzeżone”; 2) dla UE: *tres secret UE/EU top secret* – „ściśle tajne”, *secret UE/EU secret* – „tajne”, *confidentiel UE/EU confidential* – „poufne”, *restreint UE/EU restricted* – „zastrzeżone”. Informacją niejawną międzynarodową jest również polska informacja niejawna, udostępniona partnerowi zagranicznemu.

[25] Informacje niejawne mogą być wyrażone w dokumencie lub materiale i prezentowane przez okazanie bądź ustne opisanie ich treści. Dokumentem jest każda informacja niejawna utrwalona na piśmie, mikrofilmach, negatywach i fotografiach, na nośnikach danych (półprzewodnikowych, magnetycznych, optycznych), a także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej. Materiałem jest zaś zarówno dokument, jak i przedmiot, albo dowolna ich część, chroniona jako informacja niejawna, a zwłaszcza: urządzenie, wyposażenie lub broń, wyprodukowane albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia (art. 2 pkt 3 i 4 uoin). Natomiast dokumentem elektronicznym (w znaczeniu art. 3 pkt 2 uoin) jest stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.

13. Informatyczny nośnik danych – materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej[26].

14. Jednostka organizacyjna – każdy podmiot wymieniony w art. 1 ust. 2 uoin, który jest dysponentem informacji niejawnych i w którym przetwarza się informacje niejawne.

15. Klauzula tajności – to stopień niejawności informacji lub materiału (dokumentu, przedmiotu), który jednocześnie określa środki ochrony danej informacji[27].

---

[26] Informatyczne nośniki danych przeznaczone do przetwarzania informacji niejawnych obejmuje się ochroną od momentu oznaczenia nośnika klauzulą tajności aż do trwałego usunięcia danych na nim zapisanych oraz zniesienia klauzuli tajności albo do momentu jego zniszczenia. Klauzula tajności informatycznych nośników danych umożliwiających wielokrotny zapis, na których zapisano informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne", nie podlega zniesieniu lub obniżeniu; zob. § 17 ust. 1–4 Rozporządzenia w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

[27] Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. 1) Klauzulę „ściśle tajne" nadaje się informacjom niejawnym, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować wyjątkowo poważne szkody dla RP, a które dotyczą polityki międzynarodowej i obronności państwa, czynności operacyjno-rozpoznawczych służb wywiadu i kontrwywiadu, bądź też mają bezpośrednie znaczenie dla niepodległości i porządku konstytucyjnego RP. 2) Informacjom niejawnym nadaje się klauzulę „tajne", jeżeli ich nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować poważne szkody dla państwa. Zalicza się do nich informacje dotyczące ochrony suwerenności lub porządku konstytucyjnego, stosunków międzynarodowych i przygotowań obronnych lub funkcjonowania Sił Zbrojnych RP, informacji, których ujawnienie może utrudnić wykonywanie czynności operacyjno-rozpoznawczych, zakłócić funkcjonowanie organów ścigania i wymiaru sprawiedliwości albo przynieść stratę znacznych rozmiarów w interesach ekonomicznych RP. 3) Informacjom niejawnym nadaje się klauzulę „poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla państwa, przez to, że utrudni prowadzenie bieżącej polityki zagranicznej RP; utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych RP; zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli; utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za bezpieczeństwo lub podstawowe interesy RP; utrudni wykonywanie zadań organom wymiaru sprawiedliwości i służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwo obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych; zagrozi stabilności systemu finansowego RP; niekorzystnie wpłynie na funkcjonowanie gospodarki narodowej. 4) Klauzulę „zastrzeżone**"** nadaje się zaś informacjom niejawnym, którym nie nadano wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może szkodliwie wpłynąć na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych RP. Rozporządzeniem w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności wprowadzono m.in. następujące zasady oznaczania klauzul tajności: „00" – dla klauzuli „ściśle tajne"; „0" – dla klauzuli „tajne", „Pf" – dla klauzuli „poufne", i „Z" – dla klauzuli „zastrzeżone". (art. 5 ust. 1–5 uoin).

16. Kierownik jednostki organizacyjnej – ani Ustawa o ochronie informacji niejawnych, ani Kodeks pracy nie definiują tego pojęcia. Przyjmuje się jednak, że jest to osoba, której głównym zadaniem jest organizowanie i kierowanie procesem pracy podległych mu pracowników, czyli zarządzający daną jednostką zwierzchnik (burmistrz, prezydent, starosta, właściciel, szef, dowódca, komendant itp.).

17. Komórka jednostki organizacyjnej – wydzielona organizacyjnie część jednostki organizacyjnej (wydział, dział, oddział, biuro, referat lub samodzielne stanowisko pracy).

18. Kontrola stanu zabezpieczenia informacji niejawnych – to działanie uprawnionego podmiotu (ABW i SKW) polegające na: a) ustaleniu istniejącego stanu ochrony informacji niejawnych, b) ocenie zgodności stanu rzeczywistego z przepisami prawa, c) ukazaniu przyczyn niezgodności, d) sformułowaniu zaleceń w celu uniknięcia niepożądanych zjawisk, e) przedstawieniu wyników ustaleń uprawnionemu podmiotowi[28].

19. Krajowa władza bezpieczeństwa – organ właściwy do nadzorowania systemu ochrony informacji niejawnych w stosunkach RP z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych NATO, UE lub innych organizacji międzynarodowych.

20. Nieuprawnione ujawnienie informacji ma miejsce wówczas, gdy informacja posiadająca atrybut tajności zostanie przekazana (słowem, pocztą elektroniczną, na piśmie, znakiem, gestem itp.) poza krąg osób prawnie do niej dopuszczonych.

21. Nośnik informacji – przedmiot umożliwiający fizyczne zapisanie danego rodzaju informacji, a także jej późniejsze odczytanie (odtworzenie).

22. Ochrona kryptograficzna informacji niejawnych przetwarzanych w systemach teleinformatycznych polega na zastosowaniu mechanizmów gwarantujących ich poufność, integralność oraz uwierzytelnienie.

Zgodnie z postanowieniami zawartymi w art. 9 obowiązuje następujący tryb postępowania w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności: a) w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności odbiorca materiału może zwrócić się do osoby, która ją nadała, albo jej przełożonego, z wnioskiem o dokonanie stosownej zmiany; b) w przypadku odmowy dokonania zmiany lub nieudzielenia odpowiedzi w ciągu 30 dni od daty złożenia wniosku odbiorca materiału może zwrócić się odpowiednio do ABW lub SKW o rozstrzygnięcie sporu; spór, o którym mowa, ABW lub SKW winny rozstrzygnąć w terminie 30 dni od daty złożenia wniosku o rozstrzygnięcie sporu.

[28] Poza funkcjonariuszami ABW oraz żołnierzami i funkcjonariuszami SKW kontrolę stanu zabezpieczenia informacji niejawnych przeprowadza prezes Rady Ministrów – w odniesieniu do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego realizowanych przez ABW lub SKW. Zasady i zakres kontroli stanu zabezpieczenia informacji niejawnych regulują art. 10, 11 i 12 uoin. Zob. T. Szewc, *Ochrona informacji niejawnych. Komentarz*, Warszawa 2007.

23. Postępowanie sprawdzające – czynności i sprawdzenia dokonywane przez ABW albo SKW, albo pełnomocnika ochrony w celu ustalenia, czy osoba sprawdzana (ubiegająca się o dostęp do informacji niejawnych) daje rękojmię zachowania tajemnicy. Zgodnie z art. 22 ust. 1 uoin wyróżnia się:

- zwykłe postępowanie sprawdzające przeprowadzane przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „poufne";
- poszerzone postępowanie sprawdzające przeprowadzane:
  - przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne",
  - wobec pełnomocników ochrony, ich zastępców oraz kandydatów na te stanowiska,
  - wobec kierowników jednostek organizacyjnych, w których są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej,
  - wobec osób ubiegających się o dostęp do informacji niejawnych międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez RP.

Zgodnie z art. 24 ust. 2 i ust. 3 uoin w toku postępowania sprawdzającego sprawdza się, czy wobec osoby nim objętej istnieją uzasadnione wątpliwości dotyczące m.in.:

- powiązań (uczestnictwa bądź współpracy) z obcymi służbami specjalnymi, partiami politycznymi lub organizacjami przestępczymi, których działalność wymierzona jest przeciwko RP;
- czy istnieją uzasadnione wątpliwości dotyczące przestrzegania porządku konstytucyjnego RP;
- czy występują okoliczności pozwalające ją szantażować lub wywierać na nią presję;
- czy osoba sprawdzana świadomie ukryła lub podała w toku postępowania nieprawdziwe informacje mające istotne znaczenie dla ochrony informacji niejawnych;
- czy sprawdzana osoba, jeśli miała już wcześniej dostęp do informacji niejawnych, właściwie z nimi postępowała.

W toku poszerzonego postępowania sprawdzającego ustala się ponadto, czy istnieją wątpliwości dotyczące (art. 24 ust. 3 uoin):

- poziomu życia osoby sprawdzanej wyraźnie przewyższającego uzyskiwane przez nią dochody;
- choroby psychicznej lub innych zakłóceń czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpływać na zdolność osoby sprawdzanej do wykonywania prac związanych z dostępem do informacji niejawnych;
- uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych;

Zwykłe postępowanie sprawdzające przeprowadza pełnomocnik ochrony na pisemne polecenie kierownika jednostki organizacyjnej (art. 23 ust.1 uoin). Natomiast ABW albo SKW przeprowadzają poszerzone postępowanie sprawdzające (art. 23 ust. 2 uoin):

- na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska lub zlecenia prac;
- wobec funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w ABW albo SKW;
- wobec osób wykonujących czynności zlecone lub ubiegających się o wykonywanie tych czynności na rzecz ABW albo SKW.

ABW przeprowadza poszerzone postępowanie sprawdzające wobec szefa SKW, szefa AW, szefa CBA, szefa BOR-u, komendanta głównego Policji, dyrektora generalnego SWW, komendanta głównego SG oraz osób przewidzianych na te stanowiska, a także pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w SKW, AW, CBA, BOR-ze, Policji, SW oraz SG.

SKW przeprowadza zaś poszerzone postępowania sprawdzające wobec szefa ABW, szefa SWW, komendanta głównego ŻW oraz osób przewidzianych na te stanowiska, a także pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w ABW, SWW oraz ŻW.

Ponadto AW, CBA, BOR, Policja, SW, SWW, SG oraz ŻW przeprowadzają samodzielne postępowania sprawdzające oraz kontrolne postępowania sprawdzające odpowiednio wobec własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy, osób wykonujących na ich rzecz czynności zlecone lub ubiegających się o wykonywanie tych czynności.

Postępowanie sprawdzające rozpoczyna się od wypełnienia przez osobę zainteresowaną ankiety bezpieczeństwa osobowego i złożenia jej pełnomocnikowi, a kończy (zgodnie z art. 28 uoin): a) wydaniem poświadczenia bezpieczeństwa, b) decyzją o odmowie wydania poświadczenia bezpieczeństwa, c) decyzją o umorzeniu postępowania sprawdzającego. Wniosek o wszczęcie poszerzonego postępowania sprawdzającego powinien być skierowany do dyrektora Departamentu Ochrony Informacji Niejawnych ABW w przypadku zamieszkania osoby sprawdzanej w granicach administracyjnych miasta stołecznego Warszawy lub do dyrektora właściwej terytorialnie delegatury ABW w pozostałych przypadkach.

W przypadku, gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające; przeprowadza je organ właściwy do przeprowadzenia (pełnomocnik, ABW, SKW w terminie 6 miesięcy). Osoba sprawdzana nie wypełnia nowej ankiety bezpieczeństwa osobowego dla celów tego postępowania.

Kontrolne postępowanie sprawdzające kończy się: a) decyzją o cofnięciu poświadczenia bezpieczeństwa, b) poinformowaniem wnioskodawcy o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym, z jednoczesnym potwierdzeniem dalszej jej zdolności do zachowania tajemnicy w zakresie określonym w posiadanym przez nią poświadczeniu bezpieczeństwa, c) decyzją o umorzeniu postępowania, jeśli postępowanie to nie zostanie zakończone przed upływem 12 miesięcy od dnia jego wszczęcia.

24. Poświadczenie bezpieczeństwa – to dokument uprawniający jego posiadacza do dostępu do informacji niejawnych o wskazanej w nim klauzuli tajności przez okres, na jaki zostało wydane[29].

25. Przedsiębiorca – osoba fizyczna, osoba prawna i jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznaje zdolność prawną, wykonująca we własnym imieniu działalność gospodarczą, wspólnicy spółki cywilnej lub każda inna jednostka organizacyjna, które w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa (art. 2 pkt 13 uoin).

26. Przetwarzanie informacji niejawnych to wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, a w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie (art. 2 pkt 5 uoin).

27. Rękojmia zachowania tajemnicy – zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego (art. 2 pkt 2 uoin).

28. System ochrony informacji niejawnych – to zespół wzajemnie powiązanych i uzupełniających się środków, a także przedsięwzięć organizacyjnych, technicznych i prawnych uniemożliwiających nieuprawniony dostęp i nieuprawnione rozpowszechnianie informacji niejawnych[30].

---

[29] Zob. Rozporządzenie w sprawie wzorów poświadczeń bezpieczeństwa. Poświadczenia bezpieczeństwa upoważniające do dostępu do polskich informacji niejawnych upoważniają jednocześnie do dostępu do informacji niejawnych międzynarodowych (NATO i UE). Dostęp do tych informacji jest jednak uwarunkowany posiadaniem odpowiedniego poświadczenia/świadectwa NATO lub UE. W celu wydania poświadczenia bezpieczeństwa organizacji międzynarodowej nie jest wymagane wypełnienie ankiety bezpieczeństwa osobowego; dokumenty te są wydawane przez ABW, SKW, AW lub SWW na podstawie ważnego polskiego poświadczenia bezpieczeństwa lub świadectwa bezpieczeństwa przemysłowego na okres ważności posiadanego dokumentu (art. 32 ust. 4 uoin). Zgodnie z art. 34 ust. 5 pkt l uoin w szczególnie uzasadnionych przypadkach pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych o klauzuli „poufne", „tajne" lub „ściśle tajne" osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa może wyrazić: szef Kancelarii Prezydenta RP; szef Kancelarii Sejmu; szef Kancelarii Senatu; szef Kancelarii Prezesa Rady Ministrów; minister właściwy dla określonego działu administracji rządowej; prezes NBP; prezes NIK; kierownik urzędu centralnego, a w przypadku ich braku odpowiednio ABW albo SKW.

[30] Na system ochrony informacji niejawnych w RP składa się sześć elementów (podsystemów zadaniowo-funkcyjnych). Są to: 1) bezpieczeństwo osobowe, które obejmuje kwestię dostępu do informacji niejawnych i regulacje związane z prowadzeniem postępowań sprawdzających osób ubiegających się o dostęp do takich informacji, 2) szkolenia w zakresie ochrony informacji niejawnych, 3) bezpieczeństwo przemysłowe, 4) ewidencje, przechowywanie i udostępnianie akt sprawdzających, 5) kancelarie tajne i środki bezpieczeństwa fizycznego, odnoszące się do wskazań, gdzie i w jaki spo-

29. System informacyjny – to wielopoziomowa struktura organizacji, firmy lub korporacji, pozwalająca jego użytkownikowi na transformowanie określonych informacji wejściowych na pożądane informacje wyjściowe. Podstawowymi elementami systemu informacyjnego są użytkownicy systemu, informacje stanowiące zasób informacyjny, elementy i narzędzia techniczne służące gromadzeniu, przetwarzaniu, przesyłaniu i udostępnianiu informacji, a także rozwiązania systemowe i relacje między nimi zachodzące[31].

30. System informatyczny – jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. Na system informatyczny składają się: komputery, urządzenia służące do przechowywania danych, urządzenia służące do komunikacji między sprzętowymi elementami systemu, urządzenia służące do komunikacji między ludźmi a komputerami, urządzenia służące do odbierania danych ze świata zewnętrznego (czujniki elektroniczne, kamery, skanery), urządzenia służące do wpływania na świat zewnętrzny (silniki sterowane komputerowo, roboty przemysłowe, sterowniki urządzeń mechanicznych), urządzenia służące do przetwarzania danych niebędące komputerami, oprogramowanie, ludzie oraz procedury organizacyjne i elementy informacyjne (bazy wiedzy)[32].

31. System teleinformatyczny – to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną[33].

32. SZBI – to część całościowego systemu zarządzania, oparta na systematycznym podejściu do niego, oraz odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. Obejmuje on ludzi, procesy, infrastrukturę i systemy informatyczne. Wdrażany zaś i certyfikowany jest na podstawie normy ISO/IEC 27001[34].

33. Świadectwo bezpieczeństwa przemysłowego – dokument potwierdzający zdolność przedsiębiorcy do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej, wydawany przez ABW albo SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego (art. 54 ust. 2 uoin).

---

sób można przechowywać te informacje, 6) ochrona informacji niejawnych międzynarodowych.

31 Za: *Zarządzanie bezpieczeństwem informacyjnym*…, s. 5 i 79.

32 *Ibidem*, s. 80.

33 Por. art. 2 pkt 3 Ustawy o świadczeniu usług drogą elektroniczną. Według K. Lidermana (*idem*, *Bezpieczeństwo informacyjne*…, s. 30) na system teleinformatyczny składają się: 1) informacja przetwarzana, przechowywana i przesyłana w systemie, 2) sprzęt umożliwiający przetwarzanie, przechowywanie i przesyłanie informacji, 3) systemy operacyjne i oprogramowanie narzędziowe, 4) infrastruktura (budynki, źródła zasilania w energię i wodę oraz system ochrony), 5) ludzie operatorzy.

34 Obejmuje on ludzi, procesy, infrastrukturę i systemy informatyczne, a wdrażany jest oraz certyfikowany na podstawie normy ISO/IEC 27001 (PN 27001). Za: *Zarządzanie bezpieczeństwem informacyjnym*…, s. 82 i 86.

34. Zasoby (aktywa) systemu teleinformatycznego – informacje przetwarzane w systemie teleinformatycznym, a także osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji[35].

3. Podmioty administracji bezpieczeństwa informacji niejawnych

W jednostce organizacyjnej, w której są przetwarzane informacje niejawne, osobami zaangażowanymi w procesy zapewnienia ich ochrony (administratorami bezpieczeństwa) są:
a) kierownik jednostki organizacyjnej,
b) pełnomocnik do spraw ochrony informacji niejawnych,
c) inspektor bezpieczeństwa teleinformatycznego,
d) administrator systemu teleinformatycznego,
e) kierownik kancelarii tajnej[36].

Kierownik jednostki organizacyjnej
Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony (art. 14 ust. 1 uoin).

W ramach tej odpowiedzialności na kierowniku jednostki organizacyjnej spoczywają następujące obowiązki, takie jak:
- zaznajomienie podległych mu pracowników z zakresem informacji niejawnych, do których będą mieli dostęp, a także z procedurami wykonywania pracy, zapewniającymi ochronę tych informacji;
- opracowanie dokumentacji;
- wykaz stanowisk i rodzajów prac zleconych, z którymi może się wiązać dostęp do informacji niejawnych;
- szczególne wymagania bezpieczeństwa systemu lub sieci teleinformatycznej oraz procedury bezpiecznej ich eksploatacji;
- instrukcji bezpieczeństwa przemysłowego;
- prowadzenie dokumentacji osobowej osób mających dostęp do informacji niejawnych, obejmującej:
  – ankietę bezpieczeństwa osobowego,
  – poświadczenie bezpieczeństwa,

---

35 *Ibidem*, § 2 pkt 15; K. Liderman, *Bezpieczeństwo informacyjne*..., s. 132.

36 Do wymienionych osób zaangażowanych w zapewnienie bezpieczeństwa informacyjnego należy dołączyć jeszcze pracowników technicznych (pracowników kierujących działem IT, administratorów serwerów, sieci i stacji roboczych) oraz pracowników zaangażowanych organizacyjnie (kierowników komórek organizacyjnych, zespół kierowania polityką bezpieczeństwa). Za: K. Liderman, *Bezpieczeństwo informacyjne*..., s. 38.

  - potwierdzenie zapoznania się z zakresem tajemnicy prawnie chronionej na zajmowanym stanowisku i w ramach wykonywanych zadań.
- wdrażanie rozwiązań organizacyjno-technicznych przewidzianych w ustawie w celu ochrony informacji niejawnych;
- współdziałanie ze służbami i instytucjami uprawnionymi do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego.

Pełnomocnik do spraw ochrony informacji niejawnych

Pełnomocnikiem ochrony do spraw ochrony informacji niejawnych (dalej: pełnomocnik ochrony) jest osoba specjalnie zatrudniona, bezpośrednio podległa kierownikowi jednostki organizacyjnej i w pełni niezależna od pozostałych pracowników jednostki. Utworzenie stanowiska pełnomocnika ochrony jest obligatoryjne w każdej jednostce organizacyjnej, w której są przetwarzane informacje niejawne.

Pełnomocnikiem ochrony może być osoba posiadająca (art. 14 ust. 3 uoin):

a) obywatelstwo polskie,
b) wykształcenie wyższe[37],
c) odpowiednie poświadczenie bezpieczeństwa wydane przez ABW albo SKW,
d) zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych, przeprowadzonym przez ABW albo SKW.

Do zadań pełnomocnika ochrony należy (art. 15 ust. 1 i art. 23 ust. 1 uoin):

- zapewnienie przestrzegania przez pracowników jednostki organizacyjnej przepisów o ochronie informacji niejawnych;
- stosowanie środków bezpieczeństwa fizycznego;
- zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;
- analiza i zarządzanie ryzykiem bezpieczeństwa informacji niejawnych[38];

---

[37] Przepisu o wykształceniu wyższym nie stosuje się do pełnomocników ochrony zatrudnionych na stanowisku przed 2 stycznia 2011 r.

[38] Ryzyko oznacza sytuację powodującą niebezpieczeństwo lub możliwość, że zdarzy się coś złego. Według przedmiotowej ustawy ryzykiem jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji; szacowaniem ryzyka – całościowy proces analizy i oceny ryzyka, a zarządzaniem ryzykiem – skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka. (art. 2 pkt 15, 16 i 17 uoin). W ramach analizy ryzyka dokonuje się zestawienia zidentyfikowanych podatności z potencjalnymi zagrożeniami oraz skutkami wynikającymi z wystąpienia tych zagrożeń. Zarządzanie ryzykiem, związanym z przetwarzaniem informacji niejawnych, jest procesem, na który składają się przyjęte kryteria oceny ryzyka, kryteria oceny skutków, kryteria akceptacji ryzyka, zdefiniowany zakres i granice zarządzania ryzykiem oraz ustalona struktura funkcjonalna odpowiedzialna za realizację poszczególnych procedur. Gwarancją prawidłowej realizacji obowiązku ciągłości funkcjonowania procesu zarządzania ryzykiem jest postępowanie zgodnie z metodyką szacowania ryzyka określoną w normie PN ISO/IEC 27005:2010. Szerzej zob. K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.

- kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na 3 lata) kontrola ewidencji, materiałów i obiegu dokumentów;
- opracowywanie i aktualizowanie, wymagające akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej (w tym w razie wprowadzenia stanu nadzwyczajnego) i nadzorowanie jego realizacji;
- prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
- prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających[39];
- prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia dostępu do informacji niejawnych, osób, wobec których kierownik jednostki organizacyjnej wydał zgodę na udostępnienie informacji niejawnych o klauzuli „poufne" oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto[40];
- przekazywanie (odpowiednio ABW albo SKW) do ewidencji osób uprawnionych do dostępu do informacji niejawnych o klauzuli „poufne" i wyższej, a także danych osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa.

Ponadto w zależności od klauzuli przetwarzanych informacji niejawnych pełnomocnik ochrony zobligowany jest do opracowania:

---

[39] Zgodnie z pkt 11 i 12 instrukcji wypełnienia ankiety bezpieczeństwa osobowego, która stanowi załącznik do przedmiotowej ustawy, osoby objęte zwykłym postępowaniem sprawdzającym nie wypełniają części V, VI i VII ankiety. Natomiast osoby, wobec których będzie przeprowadzane poszerzone postępowanie sprawdzające do klauzuli „poufne", nie wypełniają części VII ankiety.

[40] Omawiany wykaz winien obejmować wyłącznie: imię i nazwisko, numer PESEL, imię ojca, datę i miejsce urodzenia, adres miejsca zamieszkania lub pobytu, określenie dokumentu kończącego procedurę, datę jego wydania oraz numer (art. 15 ust. 1 pkt 8 uoin). Zgodnie z art. 73 ust. 3 uoin dostęp do danych z wykazu prowadzonego przez pełnomocnika ochrony jest ograniczony. Dane te są udostępniane na pisemne żądanie wyłącznie w określonych ustawowo przypadkach i tylko określonym ustawowo podmiotom, a mianowicie: a) dla celów postępowania sprawdzającego, kontrolnego postępowania sprawdzającego oraz postępowania bezpieczeństwa przemysłowego (służbom i instytucjom uprawnionym do prowadzenia takich postępowań), b) właściwym organom w celu przeprowadzenia kontroli prawidłowości postępowania, c) dla celów postępowania odwoławczego i zażaleniowego, d) dla celów postępowania skargowego (sądowi administracyjnemu), e) dla celów postępowania karnego (sądowi, prokuratorowi). W związku z tym, że Ustawa o ochronie informacji niejawnych jest właśnie taką ustawą szczególną, bo przewiduje większy rygor ochrony danych, zastosowanie przepisów Ustawy o ochronie danych osobowych jest w tym zakresie wyłączone i nie ma obowiązku rejestrowania przedmiotowego wykazu u GIODO.

- dokumentacji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne" w podległych komórkach organizacyjnych;
- dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą[41];
- instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.

Omówione zadania pełnomocnik ochrony realizuje przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, zwanej pionem ochrony[42] (jeżeli jest ona utworzona w jednostce organizacyjnej).

W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych pełnomocnik ochrony zawiadamia o tym kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.

W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne" lub wyższej pełnomocnik ochrony zawiadamia niezwłocznie również odpowiednio ABW lub SKW (art. 17 ust. 1 i 2 uoin).

Inspektor bezpieczeństwa teleinformatycznego

Inspektor bezpieczeństwa teleinformatycznego bierze udział w procesie zarządzania ryzykiem w systemie teleinformatycznym, weryfikując:

a) poprawność realizacji zadań przez administratora, w tym właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom;
b) znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz PBE w systemie teleinformatycznym, w tym w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;
c) stan zabezpieczeń systemu teleinformatycznego, w tym rejestry zdarzeń systemu teleinformatycznego[43].

---

41 Określając poziom zagrożeń, w szczególności uwzględnia się: a) występujące rodzaje zagrożeń, b) klauzulę tajności i liczbę dokumentów niejawnych będących w dyspozycji jednostki, c) lokalizację pomieszczeń, w których są (będą) przetwarzane informacje niejawne, d) liczbę osób mających dostęp do informacji niejawnych w danej jednostce organizacyjnej, e) organizację i środki bezpieczeństwa fizycznego. W uzasadnionych przypadkach w określeniu poziomu zagrożeń uwzględnia się (obligatoryjnie) wskazania ABW lub SKW (art. 45 ust. 2 i 3 uoin).

42 Komórka ta, w różnych organach i instytucjach, nosi różne nazwy, np. może to być biuro, departament, zarząd lub wydział ochrony informacji niejawnych. Wymagania stawiane pracownikom pionu ochrony dotyczą przede wszystkim posiadania obywatelstwa polskiego, odpowiedniego poświadczenia bezpieczeństwa i zaświadczenia o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych (art. 16 uoin).

43 Specjalistyczne szkolenie z zakresu bezpieczeństwa teleinformatycznego, wspólne dla administratorów systemów oraz inspektorów bezpieczeństwa teleinformatycznego, prowadzone jest przez Departament Bezpieczeństwa Teleinformatycznego ABW w for-

Administrator systemu teleinformatycznego
Administrator systemu teleinformatycznego to osoba, lub zespół osób, odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego.

Administrator systemu teleinformatycznego bierze udział w tworzeniu dokumentacji bezpieczeństwa systemu teleinformatycznego oraz w procesie zarządzania ryzykiem w systemie teleinformatycznym:
a) realizując szkolenia użytkowników systemu teleinformatycznego;
b) utrzymując zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;
c) wdrażając zabezpieczenia w systemie teleinformatycznym.

Kierownik kancelarii tajnej
Kierownik kancelarii kieruje wyodrębnioną organizacyjnie i lokalizacyjnie komórką, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów niejawnych uprawnionym osobom (art. 42 uoin)[44].

Do podstawowych zadań kierownika kancelarii tajnej należy:
a) bezpośredni nadzór nad obiegiem materiałów;
b) udostępnianie materiałów osobom do tego uprawnionym;
c) wydawanie, za pokwitowaniem, materiałów osobom do tego uprawnionym i zapewniającym odpowiednie warunki do przechowywania tych materiałów[45];
d) egzekwowanie zwrotu materiałów;

---

mie jednodniowych zjazdów, które odbywają się w Warszawie. Udział w szkoleniu jest odpłatny (z wyłączeniem jednostek organizacyjnych Policji). Jednostka organizacyjna, chcąc skierować osobę na przeszkolenie, dokonuje pisemnego zgłoszenia kandydata, które przesyła na adres: Agencja Bezpieczeństwa Wewnętrznego, Departament Bezpieczeństwa Teleinformatycznego, Warszawa 00-993, ul. Rakowiecka 2a.

[44] Kancelarię tajną tworzy kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „tajne" lub „ściśle tajne". Kierownik jednostki organizacyjnej może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne" lub „zastrzeżone". O utworzeniu lub likwidacji kancelarii tajnej informuje się odpowiednio ABW lub SKW (art. 42 ust. 1, 5 i 6 uoin). Zgodnie z art. 43 ust. 1 uoin organizacja pracy kancelarii tajnej winna zapewnić możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „tajne" lub „ściśle tajne" oraz kto z tym materiałem się zapoznał. W tym celu kancelaria prowadzi: 1) rejestr dzienników i teczek, 2) dzienniki ewidencyjne, 3) książkę doręczeń przesyłek miejscowych, 4) wykaz przesyłek nadanych, 5) rejestr wydanych nośników informacji i innych przedmiotów oraz karty zapoznania się z dokumentem (§ 2 ust. 2 oraz § 7 ust. 2 Rozporządzenia w sprawie organizacji i funkcjonowania kancelarii tajnych.

[45] W celu realizacji tego zadania kierownik kancelarii powinien mieć dostęp do wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które mają uprawnienia dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto.

e) kontrola przestrzegania właściwego oznaczania[46] i rejestrowania materiałów w kancelarii oraz jednostce organizacyjnej[47];
f) zgodne z obowiązującymi przepisami przyjmowanie i nadawanie przesyłek zawierających informacje niejawne[48];
g) nadzór nad pracą oddziałów kancelarii[49].

4. Zasady i procedury organizacji ochrony informacji niejawnych

1. Ochronie podlegają wszystkie informacje niejawne, niezależnie od formy i sposobu ich wyrażenia, a także będące w stadium opracowania.
2. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku (art. 4 ust. 1 uoin).
3. Informacje niejawne, którym nadano określoną klauzulę tajności mogą być udostępniane wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności (art. 8 pkt 1 uoin).
4. Dopuszczenie do pracy lub pełnienia służby na stanowiskach związanych z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej może

---

[46] Zgodnie z § 2 pkt 1 Rozporządzenia w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności przez oznaczanie należy rozumieć czynność techniczną nanoszenia na materiał klauzuli tajności, numeru egzemplarza, numeru strony i innych informacji przewidzianych w tym rozporządzeniu. Czynności tej nie należy mylić z czynnością nadawania klauzuli tajności na podstawie spełnienia ustawowych przesłanek przez osobę uprawnioną do podpisania dokumentu. Jeśli jednak kierownik kancelarii, zastępca kierownika lub osoba kierująca oddziałem kancelarii jest odbiorcą materiału, może skorzystać z prawa określonego w art. 9 uoin – poinformować pełnomocnika ochrony o zawyżeniu lub zaniżeniu klauzuli tajności materiału

[47] Rozporządzenie w sprawie organizacji i funkcjonowania kancelarii tajnych wprowadza bezwzględny nakaz niezwłocznego rejestrowania otrzymanego, wysłanego, lub wytworzonego materiału niejawnego w odpowiednim dzienniku lub rejestrze (§ 7 ust. 1 i § 9 ust. 1). W przypadku przyjęcia dokumentów do kancelarii tajnej rejestrację powinien przeprowadzić kierownik kancelarii lub inny upoważniony pracownik.

[48] Szczegółowe procedury z tym związane reguluje Rozporządzenie w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne.

[49] Ze względu na charakter i specyfikę procesów przetwarzania informacji niejawnych kierownik jednostki organizacyjnej może podjąć decyzję o utworzeniu więcej niż jednej kancelarii tajnej funkcjonującej na jego potrzeby. Kierowanie oddziałem kancelarii tajnej powierza się – na podstawie decyzji pełnomocnika ochrony – pracownikowi pionu ochrony, który w zakresie funkcjonowania oddziału realizuje obowiązki kierownika kancelarii. Ustawodawca dopuszcza również działanie jednej kancelarii tajnej obsługującej kilka podmiotów. W tym przypadku wymagana jest akceptacja tego rozwiązania przez ABW lub SKW (art. 42 ust. 2 i 3 uoin).

nastąpić wyłącznie odnośnie do osób posiadających poświadczenie bezpieczeństwa oraz przeszkolonych w zakresie ochrony informacji niejawnych.

Dokumentami uprawniającymi do dostępu do informacji niejawnych o klauzuli „zastrzeżone" są: pisemne upoważnienie kierownika jednostki organizacyjnej (jeżeli dana nie posiada poświadczenia bezpieczeństwa) oraz zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych (art. 21 ust. 4 pkt 1 uoin)[50].

5. Poświadczenia bezpieczeństwa są wydawane na określony czas (art. 29 ust. 3 uoin):
   a) 10 lat – w przypadku dostępu do informacji niejawnych o klauzuli „poufne";
   b) 7 lat – w przypadku dostępu do informacji niejawnych o klauzuli „tajne";
   c) 5 lat – w przypadku dostępu do informacji niejawnych o klauzuli „ściśle tajne"[51].
6. Zgodnie z art. 23 ust. 5 uoin AW, CBA, BOR, Policja, SW, SWW, SG oraz ŻW przeprowadzają samodzielnie postępowania sprawdzające (zwykłe i poszerzone) oraz kontrolne postępowania sprawdzające wobec:
   a) własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy;
   b) osób wykonujących na ich rzecz czynności zlecone lub ubiegających się o wykonywanie tych czynności[52].
7. W szczególnie uzasadnionych przypadkach pisemną zgodę na jednorazowe udostępnienie określonych materiałów niejawnych o klauzuli „poufne", „taj-

---

[50] Treść art. 21 ust. 4 pkt 1 uoin nie wskazuje wprost, jakie elementy powinno zawierać owe pisemne upoważnienie, ale mając na względzie art. 29 ust. 1 uoin, można mniemać, iż powinny się w nim znaleźć takie dane, jak: nazwa jednostki organizacyjnej, data i miejsce wydania, podstawa prawna, imię (imiona), nazwisko, PESEL i imię ojca osoby upoważnionej, cel wydania i czas ważności upoważnienia, pieczątka i podpis kierownika jednostki organizacyjnej. W przypadku prac lub zadań zleconych bądź udziału w spotkaniu z dostępem do informacji o klauzuli „zastrzeżone" upoważnienie, o którym mowa, wydaje kierownik przedsiębiorcy przyjmującego zlecenie lub kierownik jednostki delegującej do udziału w spotkaniu. Treść art. 21 nie wskazuje również wprost, na jaki okres wydaje się pisemne upoważnienie kierownika jednostki organizacyjnej, pozostawiając to w zakresie jego uprawnień. Dlatego też możliwe jest wydanie takiego upoważnienia: a) w konkretnym celu (np. wykonania określonego zadania), b) na czas określony konkretnym przedsięwzięciem (np. datą od do), c) zapisem: „do odwołania" lub „na czas zatrudnienia w jednostce organizacyjnej.

[51] Wzory poświadczeń bezpieczeństwa, decyzji o odmowie ich wydania oraz decyzji o cofnięciu poświadczenia bezpieczeństwa stanowią załączniki do rozporządzeń Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. (Dz.U. z 2010 r. Nr 258, poz. 1752, 1753 i 1754). Zgodnie z art. 29 ust. 4 uoin poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych wyższej klauzuli tajności uprawnia do dostępu do informacji niejawnych o niższej klauzuli tajności, odpowiednio przez okresy, na jakie je wydano.

[52] Zgodnie z art. 29 ust. 5 uoin poświadczenia bezpieczeństwa wydane dla osób wymienionych w pkt „a" i „b" zachowują ważność wyłącznie w okresie pracy lub służby w organie, który je wystawił.

ne" lub „ściśle tajne" osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa może wyrazić (art. 34 ust. 5 pkt 1 uoin):
   a) szef Kancelarii Prezydenta RP,
   b) szef Kancelarii Sejmu,
   c) szef Kancelarii Senatu,
   d) szef Kancelarii Prezesa Rady Ministrów,
   e) minister właściwy dla określonego działu administracji rządowej,
   f) prezes NBP,
   g) prezes NIK,
   h) kierownik urzędu centralnego, a w przypadku ich braku odpowiednio ABW albo SKW.
8. Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli ich tajności (art. 6 ust. 2 uoin).
9. Zniesienie lub zmiana klauzuli tajności jest możliwa wyłącznie po wyrażeniu pisemnej zgody przez osobę, która była upoważniona do jej nadania, bądź jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony (art. 6 ust. 3 uoin)[53].
10. Ochronie bezterminowej podlegają dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych (np. Policji, ABW, AW, SKW, SWW, CBŚ, b. UOP), a także informacje uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia (Interpol, Europol, CIA, FBI, DEA, BND itp.)[54].

---

[53] Zgoda na zniesienie lub zmianę klauzuli tajności powinna być utrwalona w postaci odpowiednich adnotacji – na dokumencie nieelektronicznym, w metryce dokumentu – w dokumencie elektronicznym lub w odrębnym dokumencie podlegającym rejestracji. Na poziomie edycji dokumentu zniesienie klauzuli tajności w przypadku dokumentu nieelektronicznego polega na skreśleniu wszystkich oznaczeń znoszonej klauzuli, a nad pierwszą w kolejności skreśloną klauzulą tajności umieszcza się napis: „zniesiono klauzulę tajności" wraz z datą, imieniem i nazwiskiem oraz podpisem osoby wprowadzającej zmianę. Zmiana klauzuli tajności obejmuje analogiczne czynności. Uprawnienia w zakresie zniesienia lub zmiany klauzuli tajności materiału przechodzą, w przypadku rozwiązania, zniesienia, likwidacji, upadłości obejmującej likwidację majątku upadłego, przekształcenia lub reorganizacji jednostki organizacyjnej, na jej następcę prawnego. W przypadku braku następcy prawnego – na ABW lub SKW (art. 6 ust. 7 uoin). Skreślenia i wszelkie adnotacje powinny być wprowadzone przez kierownika kancelarii, kierownika archiwum lub kierownika innej niż kancelaria tajna komórki organizacyjnej, czytelnie i kolorem czerwonym. Niedozwolone są wszelkie korekty nadanych klauzul tajności przez wycieranie, wywabianie lub zamazywanie (§ 13 ust. 3 i 4 Rozporządzenia w sprawie oznaczania materiałów i umieszczania na nich klauzul tajności).

[54] Art. 7 ust. 1, pkt 1, 2 i 3 uoin. Ochronie nie podlegają dane, o których mowa, zawarte w dokumentach, zbiorach danych, rejestrach i kartotekach, a także w aktach funkcjonariuszy i żołnierzy organów bezpieczeństwa państwa z lat 1944–1990, będących w dyspozycji Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (*ibidem*, ust. 2).

11. Informacje niejawne muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności (art. 8 pkt 2 uoin).
12. Informacje niejawne, którym nadano określoną klauzulę tajności, muszą być chronione odpowiednio do nadanej klauzuli i z zastosowaniem określonych środków bezpieczeństwa (art. 8 pkt 3 uoin)[55].
13. Do niewłaściwego postępowania z informacjami niejawnymi dochodzi, jeżeli (art. 24 ust. 2 pkt 6 uoin):
    a) doprowadziło to bezpośrednio do ujawnienia informacji niejawnych osobom nieuprawnionym;
    b) było wynikiem celowego działania;
    c) stwarzało realne zagrożenie ich nieuprawnionym ujawnieniem i nie miało charakteru incydentalnego;
    d) dopuściła się tego osoba szczególnie zobowiązana do ochrony informacji niejawnych na podstawie ustawy (pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej).
14. Za ochronę informacji niejawnych odpowiedzialny jest kierownik jednostki organizacyjnej, w której takie informacje są wytwarzane, przetwarzane lub przechowywane (art. 14 ust. 1 uoin).
15. Szkolenia w zakresie ochrony informacji niejawnych przeprowadza się wobec:
    a) osób ubiegających się o dostęp do takich informacji;
    b) osób posiadających dostęp do takich informacji – nie rzadziej niż raz na 5 lat (art. 19 ust. 3 uoin)[56].
16. Osoby nieposiadające obywatelstwa polskiego nie mogą być dopuszczone do pracy lub pełnienia służby na stanowiskach albo wykonywania czynności zle-

---

[55] Kryteria i sposób określenia poziomu zagrożenia oraz dobór środków bezpieczeństwa fizycznego odpowiednich do określonego poziomu zagrożeń określa Rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

[56] Zgodnie z art. 19 uoin szkolenie, o którym mowa, przeprowadzają odpowiednio: ABW lub SKW dla pełnomocników ochrony i ich zastępców oraz osób przewidzianych na te stanowiska, przedsiębiorców wykonujących działalność jednoosobowo, a także dla kierowników przedsiębiorców, u których nie zatrudniono pełnomocników ochrony; ABW lub SKW, wspólnie z pełnomocnikiem ochrony, dla kierownika jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „ściśle tajne" lub „tajne"; pełnomocnik ochrony – dla pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej; ABW – dla posłów i senatorów. Szkolenie kończy się wydaniem zaświadczenia według wzoru załączonego do Rozporządzenia w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych. Zwolnieni z obowiązku poddania się szkoleniu są jedynie: prezydent RP, prezes Rady Ministrów oraz marszałkowie Sejmu i Senatu, a także sędziowie, prokuratorzy i ławnicy

conych, z którymi łączy się dostęp do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" (art. 21 ust. 2 uoin).

17. Zgodnie z art. 21 ust. 3 uoin osoby nieposiadające obywatelstwa polskiego mogą mieć dostęp do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne", gdy:
    a) zajmują stanowiska związane z kierowaniem wykonywania przez przedsiębiorcę umowy związanej z dostępem do informacji niejawnych lub związane z bezpośrednim wykonywaniem takiej umowy albo wykonujących zadania na rzecz obronności lub bezpieczeństwa państwa, związane z dostępem do informacji niejawnych u przedsiębiorcy;
    b) w imieniu przedsiębiorcy, o którym mowa w pkt a, uczestniczą w czynnościach zmierzających do zawarcia umowy, jeżeli czynności te są związane z dostępem do informacji niejawnych;
    c) są zatrudnione w pionie ochrony przedsiębiorcy, z wyjątkiem osoby zajmującej stanowisko pełnomocnika ochrony oraz jego zastępcy[57].
18. W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej organizuje się strefy ochronne[58].
19. Miejscem przetwarzania materiałów niejawnych jest kancelaria tajna. Stanowi ją wyodrębniona komórka organizacyjna i lokalizacyjna, odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów niejawnych uprawnionym do tego osobom[59].

---

[57] Z powyższego należy wnioskować, iż w przypadku dostępu do klauzuli „poufne" i „zastrzeżone" wymóg posiadania obywatelstwa polskiego nie występuje.

[58] Strefa ochronna to wydzielona część obiektu lub cały budynek, a także pomieszczenie wyposażone lub zabezpieczone w odpowiednie środki bezpieczeństwa fizycznego, które będą poddane kontroli wejść i wyjść, a poruszanie się w nich będzie możliwe za pomocą przepustek, identyfikatorów lub danych biometrycznych. Zgodnie z Rozporządzeniem w sprawie środków bezpieczeństwa stosowanych do zabezpieczenia informacji niejawnych tworzy się następujące strefy ochronne: 1) strefę ochronną I – obejmującą pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne" lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji, 2) strefę ochronną II – obejmującą pomieszczenie lub obszar, w którym informacje o klauzuli „poufne" i wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji, 3) strefę ochronną III – obejmującą pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów, 4) specjalną strefę ochronną – umiejscowioną w obrębie strefy ochronnej I lub strefy ochronnej II, chronioną przed podsłuchem, wyposażoną w system sygnalizacji włamania i napadu, chronioną podczas posiedzeń niejawnych, podlegającą regularnym inspekcjom (nie rzadziej niż raz w roku, po każdym nieuprawnionym wejściu lub podejrzeniu wejścia do niej), oraz w której nie ma linii komunikacyjnych, telefonów, sprzętu elektrycznego lub elektronicznego.

[59] Kancelaria taka powinna mieścić się w wyodrębnionym pomieszczeniu oraz zabezpieczonym zgodnie z przepisami i środkami ochrony, zawartymi w Rozporządzeniu w sprawie organizacji i funkcjonowania kancelarii tajnych oraz w Rozporządzeniu w sprawie

20. Jeżeli dla obsługi informacji niejawnych międzynarodowych konieczne jest utworzenie odrębnego systemu kancelaryjnego, tworzy się oddzielną kancelarię tajną międzynarodową[60].
21. System kancelarii tajnych międzynarodowych składa się z dwóch elementów:
    a) głównej kancelarii tajnej międzynarodowej dla sfery cywilnej,
    b) głównej kancelarii tajnej międzynarodowej dla sfery wojskowej,
    c) głównej kancelarii ATOMAL,
    d) kancelarii tajnych międzynarodowych,
    e) punktów kontroli informacji niejawnych międzynarodowych[61].
22. Dokument, który nie jest przewidziany do dalszego wykorzystania, o ile nie stanowi materiału archiwalnego, może zostać zniszczony (§ 10 ust. 1 Rozporządzenia w sprawie organizacji i funkcjonowania kancelarii tajnych)[62].

5. Zarządzanie bezpieczeństwem informacji

Jednostka organizacyjna pragnąca należycie zabezpieczyć swoje aktywa informacyjne winna zarządzać nimi w sposób systemowy i kompleksowy z wykorzystaniem różnych metodyk i norm (krajowych i międzynarodowych).

SZBI obejmuje całościowo wszelkie wewnętrzne i zewnętrzne zagrożenia[63] i składa się z wielu dokumentacji, w tym:

środków bezpieczeństwa stosowanych do zabezpieczenia informacji niejawnych. Obowiązek organizacji kancelarii tajnych mają jedynie jednostki organizacyjne dysponujące informacjami oznaczonymi klauzulami „ściśle tajne" i „tajne" (art. 42 uoin). W uzasadniających przypadkach można zorganizować kancelarię tajną obsługującą dwie lub więcej jednostek organizacyjnych. Kierownik jednostki organizacyjnej ma obowiązek informowania, odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej.

60 Wytyczne Agencji Bezpieczeństwa Wewnętrznego Krajowej Władzy Bezpieczeństwa z dnia 31 grudnia 2010 r.

61 *Ibidem*, pkt 26–28. Kancelarie ATOMAL – miejsca przechowywania materiałów o tematyce nuklearnej lub kryptograficznej.

62 Zniszczenia dokonuje się w taki sposób, aby niemożliwe było całkowite lub częściowe odtworzenie jego treści. Dokumenty o klauzuli „ściśle tajne" lub „tajne" powinny być niszczone przez pracownika kancelarii tajnej w obecności świadka posiadającego uprawnienia dostępu do informacji niejawnych o klauzuli co najmniej równej klauzuli tajności niszczonego dokumentu. Zniszczenie dokumentów powinno być potwierdzone protokołem zniszczenia potwierdzonym podpisami osób uczestniczących w niszczeniu. Po protokolarnym zniszczeniu dokumentu uzupełnia się rejestry, dzienniki i inne informacje o jego rejestracji adnotacją o zniszczeniu (§ 10, ust. 3 rozp.).

63 Zagrożenia – potencjalne przyczyny niepożądanego zdarzenia, które mogą spowodować szkodę w zasobach systemu informacyjnego (informatycznego). W literaturze przedmiotu wyróżnia się następujące rodzaje zagrożeń: tradycyjne (szpiegostwo, dywersja, sabotaż oraz związane z umyślnym lub nieumyślnym zachowaniem człowieka), losowe (wszelkiego rodzaju klęski żywiołowe, katastrofy, awarie, wypadki itp.), technologiczne – związane z przetwarzaniem informacji w urządzeniach i sieciach teleinformatycznych) oraz odnoszące się do praw obywatelskich (ingerencja służb specjalnych, ograniczanie jawności życia publicznego). Szerzej zob. P. Bączek, *Zagrożenia informacyjne*..., s. 77–145.

- PBI[64];
- procedur i regulacji wewnątrz jednostkowych;
- instrukcji, zarządzeń i postępowania z systemami informatycznymi;
- instrukcji odtworzenia środowiska po wystąpieniu incydentów związanych z bezpieczeństwem informacji[65];
- spisu zasobów informatycznych;
- dokumentu określającego podatność systemu na incydenty bezpieczeństwa (poziom zagrożenia nieuprawnionym ujawnieniem[66]), wnioski z analizy i oszacowania ryzyka oraz sposoby postępowania w sytuacjach kryzysowych.

Przy budowie SZBI, który uwzględnia standardy przyjęte przez NATO i UE, szczególnie przydatne są normy ISO (zob. przypis 17). Aktualnie najpopularniejszymi standardami bezpieczeństwa informacji są: norma PN ISO/IEC 17799:2007 – Technika informatyczna – Technika bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji, norma PN ISO/IEC 27001:2007 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. Wymagania oraz norma PN ISO/IEC 27005:2010 – Technika informatyczna – Techniki w bezpieczeństwie informacji. Normy te są zbiorami wytycznych pozwalających na wdrożenie efektywnego SZBI we wszystkich jednostkach organizacyjnych, przy czym każda z nich określa własne wymagania i oszacowuje prawdopodobieństwo oraz skutki wystąpienia niepożądanego zdarzenia/ryzyka.

Jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji w szczególności chroniących przed:

1) działaniem obcych służb specjalnych;

---

64 PBI to dokument zawierający wiele zaleceń oraz jasno sprecyzowanych zadań i procedur, według których dana organizacja buduje, zarządza oraz udostępnia swoje zasoby informacyjne i informatyczne. PBI określa również obowiązki użytkowników systemu lub sieci informatycznych oraz pracowników mających do nich dostęp. Zob. A. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Gliwice 2006. PBI dotyczy całego procesu korzystania z informacji, tj. zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania, a także wszystkich systemów jej przetwarzania, zarówno klasycznych (archiwów, kartotek, dokumentów papierowych), jak i systemów komputerowych. Na podstawie literatury przedmiotu można podzielić politykę bezpieczeństwa informacji na trzy obszary, które się wzajemnie przenikają i uzupełniają, a mianowicie: politykę organizacyjną, politykę ochrony technicznej i politykę personalną. W zależności od wielkości organizacji obszary te mogą być zarządzane w różnych komórkach.

65 Incydent bezpieczeństwa to pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które zagrażają ich poufności, integralności i dostępności.

66 Poziom zagrożenia określa się w trzystopniowej skali: wysoki, średni albo niski, dla pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne. Podstawowe kryteria i sposób określania poziomu zagrożeń zawiera załącznik nr 1 do Rozporządzenia w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

2) zamachem terrorystycznym[67] lub sabotażem[68];
3) kradzieżą lub zniszczeniem materiału;
4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;
5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności, niewynikającym z posiadanych uprawnień.

Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą. Przy określaniu poziomu zagrożeń, o którym mowa, uwzględnia się w szczególności występujące rodzaje zagrożeń, klauzule tajności i liczbę informacji niejawnych. W uzasadnionych przypadkach przy określaniu poziomu zagrożeń uwzględnia się wskazania odpowiednio ABW lub SKW.

W zależności od poziomu zagrożenia, określonego w wyniku przeprowadzonej analizy, do ochrony informacji niejawnych wykorzystuje się następujące środki i mechanizmy[69]:

a) personel bezpieczeństwa – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych (w tym kontrole dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na incydenty bezpieczeństwa, alarmy i sygnały);

---

[67] Obowiązujący polski Kodeks karny nie posługuje się pojęciem terroru i terroryzmu. Używa jedynie pojęcia przestępstwa o charakterze terrorystycznym, które przedstawiono w rozdziale XIV *Objaśnienie wyrażeń ustawowych* – art. 115 § 20: „Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat popełniony w celu: 1) poważnego zastraszenia wielu osób, 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu".

[68] Według *Słownika współczesnego języka polskiego* sabotaż to: 1) celowe dezorganizowanie pracy (np. niszczenie narzędzi, maszyn, spowolnienie produkcji, wykonywanie wadliwych wyrobów) mające osłabić przeciwnika; dywersja, 2) tajne, podstępne działanie mające utrudnić lub uniemożliwić realizację jakiegoś planu. W obowiązującym w Polsce Kodeksie karnym penalizowany jest jedynie sabotaż komputerowy. Zgodnie z art. 269 § 1 kk polega on na niszczeniu, uszkadzaniu, usuwaniu lub zmianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Sabotaż komputerowy zagrożony jest karą pozbawienia wolności od pół roku do 8 lat.

[69] Rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

b) bariery fizyczne – środki chroniące granice miejsc, w których są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;
c) szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;
d) mechanizmy kontroli dostępu – obejmujące elektroniczny system pomocniczy lub rozwiązania organizacyjne stosowane w celu zagwarantowania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie osobom posiadającym odpowiednie uprawnienia;
e) system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;
f) system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;
g) system kontroli osób i przedmiotów – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

6. Bezpieczeństwo teleinformatyczne

Przetwarzanie krajowych informacji niejawnych w systemach teleinformatycznych[70]

Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym osiąga się przez:

a) objęcie systemu teleinformatycznego procesem zarządzania ryzykiem dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym, zwanego dalej zarządzaniem ryzykiem w systemie teleinformatycznym;
b) ograniczenie zaufania, polegające na traktowaniu innych systemów teleinformatycznych jako potencjalnych źródeł zagrożenia oraz wdrożeniu w systemie teleinformatycznym zabezpieczeń kontrolujących wymianę informacji z tymi systemami teleinformatycznymi;

[70] Opracowano na podstawie takich dokumentów, jak: 1) Rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego; 2) Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych; 3) Decyzja Nr 17/MON w sprawie organizacji ochrony systemów teleinformatycznych.

c) wprowadzenie wielopoziomowej ochrony systemu teleinformatycznego, polegającej na stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu teleinformatycznego w celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia skutkuje naruszeniem poufności, integralności i dostępności tych informacji;
d) wykonywanie okresowych testów bezpieczeństwa;
e) ograniczanie uprawnień, polegające na nadawaniu użytkownikom systemu teleinformatycznego wyłącznie uprawnień niezbędnych do wykonywania pracy;
f) minimalizację funkcjonalności, polegającą na instalowaniu, uaktywnianiu i wykorzystywaniu w systemie teleinformatycznym wyłącznie funkcji, protokołów komunikacyjnych i usług niezbędnych do prawidłowej realizacji zadań, do których system teleinformatyczny został przeznaczony.

Przed dopuszczeniem osób do pracy w systemie teleinformatycznym kierownik jednostki organizacyjnej zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego oraz zapoznanie z PBE w zakresie, jaki ich dotyczy.

1. W celu zapewnienia ochrony przed nieuprawnionym dostępem do systemu teleinformatycznego:
   a) ustala się warunki i sposób przydzielania użytkownikom uprawnień do pracy w systemie teleinformatycznym;
   b) chroni się informacje i materiały umożliwiające dostęp do systemu teleinformatycznego;
   c) chroni się elementy systemu teleinformatycznego istotne dla jego bezpieczeństwa oraz wdraża się je w sposób zapewniający możliwość wykrycia wprowadzenia nieuprawnionych zmian lub prób ich wprowadzenia.
2. W celu niedopuszczenia do utraty poufności informacji niejawnych na skutek wykorzystania elektromagnetycznej emisji ujawniającej, która pochodzi z elementów systemu, w systemie teleinformatycznym przetwarzającym informacje niejawne o klauzuli „poufne" lub wyższej stosuje się środki ochrony elektromagnetycznej, dobierane na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych (z uwzględnieniem zaleceń), w szczególności certyfikowane urządzenia lub narzędzia kryptograficzne.
3. W celu niedopuszczenia do utraty dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych na skutek zakłócania ich pracy za pomocą emisji lub impulsów elektromagnetycznych o dużej mocy:
   a) stosuje się środki ochrony elektromagnetycznej dobierane na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych,
   b) ustala się zasady tworzenia i przechowywania kopii zapasowych, procedury postępowania w sytuacjach kryzysowych, w tym w przypadkach awarii elementów systemu teleinformatycznego oraz procedury monitorowania stanu technicznego systemu teleinformatycznego.

Akredytacja bezpieczeństwa systemu teleinformatycznego przetwarzającego krajowe informacje niejawne

Systemy teleinformatyczne, w których mają być przetwarzane krajowe informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego udzielanej na czas określony, nie dłuższy niż 5 lat (art. 48 ust. 1 i 2 uoin).

- Systemy teleinformatyczne przeznaczone do przetwarzania krajowych informacji niejawnych o klauzuli „zastrzeżone" są akredytowane przez kierownika jednostki organizacyjnej przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego (art. 48 ust. 9 uoin)[71], którą stanowią:
  - dokument SWB[72];
  - dokument PBE[73].
- Podstawą dokonywania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie (art. 49 ust. 4 uoin).

---

[71] W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", kierownik jednostki organizacyjnej przekazuje odpowiednio ABW lub SKW dokumentację bezpieczeństwa akredytowanego przez siebie systemu teleinformatycznego. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW albo SKW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zaleceń informuje odpowiednio ABW lub SKW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW albo SKW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego (art. 48 ust. 11 i 12 uoin).

[72] Dokumentem SWB systemu teleinformatycznego jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego. Dokument ten powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument SWB. Dokument SWB opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW albo SKW, bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym (art. 49 ust. 1–8 uoin).

[73] Dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu i pracowników mających do niego dostęp. Dokument procedur bezpiecznej eksploatacji opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

- Systemy teleinformatyczne przeznaczone do przetwarzania krajowych informacji niejawnych o klauzuli „poufne" lub wyższej są akredytowane przez ABW lub SKW (art. 48 ust. 3 uoin)[74].
- Proces udzielania przez ABW akredytacji bezpieczeństwa teleinformatycznego systemowi teleinformatycznemu przeznaczonemu do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej składa się z takich etapów, jak:
  - dokonanie przez ABW oceny dokumentacji bezpieczeństwa systemu teleinformatycznego;
  - złożenie do ABW wniosku o przeprowadzenie audytu bezpieczeństwa systemu teleinformatycznego;
  - przeprowadzenie przez ABW audytu bezpieczeństwa systemu teleinformatycznego;
  - wydanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego[75].
- Podstawą do wydania przez ABW świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego jest (art. 48 ust. 6 uoin):
  - zatwierdzona przez ABW dokumentacja bezpieczeństwa systemu teleinformatycznego;
  - wyniki audytu bezpieczeństwa systemu teleinformatycznego prowadzonego przez ABW, weryfikującego poprawność realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa, przy czym dla systemu przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" ABW może odstąpić od przeprowadzenia takiego audytu (art. 48 ust. 6 i ust. 8 uoin).
- Dokumentacja bezpieczeństwa systemów teleinformatycznych (SWB i PBE), przeznaczonych do przetwarzania krajowych informacji niejawnych, oraz wnioski powinny być kierowane do właściwych terytorialnie jednostek organizacyjnych ABW (właściwych delegatur ABW lub Departamentu Bezpieczeństwa Teleinformatycznego ABW dla obszaru miasta stołecznego Warszawy).

---

[74] ABW albo SKW udziela albo odmawia udzielenia akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej w terminie 6 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 6 miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie (art. 48 ust. 4 uoin).

[75] Świadectwo akredytacji bezpieczeństwa teleinformacyjnego powinno zawierać: 1) oznaczenie organu, 2) datę wydania, 3) oznaczenie podmiotu podlegającego akredytacji, 4) oznaczenie przedmiotu podlegającego akredytacji, 5) podstawę prawną, 6) rozstrzygnięcie oraz uzasadnienie faktyczne i prawne, 7) wskazanie okresu ważności akredytacji, 8) podpis, z podaniem imienia i nazwiska oraz stanowiska osoby upoważnionej do jego wydania (art. 48 ust. 7 uoin; załącznik do Rozporządzenia w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego).

- Za przeprowadzenie czynności związanych z udzielaniem przez ABW albo SKW akredytacji, określonych w art. 48 ust. 3–6 uoin, pobierane są opłaty, z zastrzeżeniem art. 53 ust. 2–3 uoin. Wysokość opłat uregulowana została Rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r. Nr 159, poz. 949), wydanym na podstawie art. 53 ust. 4 uoin.
- Obowiązkowi akredytacji nie podlegają systemy teleinformatyczne znajdujące się poza strefami ochronnymi oraz służące do pozyskiwania i przekazywania w sposób niejawny informacji oraz utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty – ABW, SKW, Policję, CBA, SG, ŻW, organy kontroli skarbowej (art. 51 ust. 1 uoin).
- Z obowiązku akredytacji są również wyłączone systemy teleinformatyczne, urządzenia lub narzędzia kryptograficzne wykorzystywane przez służby wywiadowcze (AW, SWW) poza granicami RP podczas wykonywania czynności operacyjno-rozpoznawczych oraz wydzielone stanowiska na terytorium RP służące tym służbom do odbierania i przetwarzania tych informacji (art. 51 ust. 2 uoin).

Akredytacja systemów i przetwarzanie informacji niejawnych międzynarodowych

Szef ABW pełniący funkcję krajowej władzy bezpieczeństwa realizuje również zadania w zakresie bezpieczeństwa systemów teleinformatycznych, przeznaczonych do przetwarzania informacji niejawnych międzynarodowych. Podstawowe zasady dotyczące akredytacji systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych są następujące[76]:

1. Informacje niejawne międzynarodowe mogą być przetwarzane tylko w systemach, które posiadają właściwą akredytację bezpieczeństwa teleinformatycznego.
2. Akredytacji punktów dostępowych systemów przetwarzających niejawne informacje międzynarodowe, organizowanych przez podmioty międzynarodowe, dokonuje odpowiednio, zgodnie z właściwością rzeczową, szef ABW lub szef SKW.
3. Akredytacja systemów organizowanych przez polskie jednostki organizacyjne, w których dopuszczono przetwarzanie informacji niejawnych międzynarodowych, odbywa się z uwzględnieniem postanowień lit. B i wymagań wynikających z umów międzynarodowych.

---

[76] Według: Informacje niejawne – Bezpieczeństwo teleinformatyczne (zakładka), www.bip.abw.gov.pl/portal/bip; Zarządzenie Nr 45 szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 17 sierpnia 2012 r. w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych.

Natomiast zasady akredytacji systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych, organizowanych przez polskie jednostki organizacyjne, to:

1. W przypadku systemów narodowych przeznaczonych do przetwarzania wyłącznie informacji niejawnych międzynarodowych, akredytacji udziela ABW lub SKW po potwierdzeniu wymagań wynikających z regulacji międzynarodowych.
2. W przypadku systemów narodowych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych, warunkiem udzielenia przez ABW lub SKW akredytacji dopuszczającej do ich przetwarzania jest wcześniejsze udzielenie przez kierownika jednostki organizującej systemu akredytacji bezpieczeństwa teleinformatycznego w trybie art. 48 ust. 9 lub 10 uoin.
3. W ciągu 30 dni od udzielenia akredytacji, o której mowa w pkt 2, kierownik jednostki organizującej system zobowiązany jest przesłać do ABW lub SKW dokumentację bezpieczeństwa systemu teleinformatycznego.
4. W przypadku systemów narodowych, w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych, dokumentacja, o której mowa w pkt 3, uwzględniająca wymagania wynikające z regulacji międzynarodowych, przesyłana jest razem z pisemnym wnioskiem o udzielenie przez ABW lub SKW akredytacji w zakresie przetwarzania informacji międzynarodowych.
5. Akredytacji systemu, o której mowa w pkt 4, udziela się wyłącznie po potwierdzeniu przez ABW lub SKW spełnienia przez system wymagań wynikających z regulacji międzynarodowych.
6. Potwierdzeniem udzielenia akredytacji, o których mowa w pkt 2 i 5, są:
   a) w odniesieniu do informacji niejawnych narodowych – zatwierdzona przez kierownika jednostki organizującej system dokumentacja bezpieczeństwa systemu oraz brak zaleceń lub potwierdzenie usunięcia zaleceń ABW lub SKW (zgodnie z art. 48 ust. 12 uoin);
   b) w odniesieniu do informacji niejawnych międzynarodowych – pisemne potwierdzenie udzielenia przez ABW lub SKW akredytacji określające:
      – zakres akredytacji (akredytowane elementy systemu, klauzule informacji itp.);
      – datę ważności akredytacji;
      – warunki utrzymywania ważności akredytacji.
   c) w przypadku systemów narodowych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej, w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych:
      – możliwe jest równoległe prowadzenie przez ABW lub SKW procesów akredytacji dla informacji krajowych i międzynarodowych;
      – akredytacji systemu dla informacji międzynarodowych udziela się wyłącznie po potwierdzeniu przez ABW lub SKW spełnienia przez system wymagań wynikających z regulacji międzynarodowych;

- potwierdzeniem udzielenia akredytacji dla informacji krajowych jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego, o którym mowa w art. 48 ust. 5 uoin;
- potwierdzeniem udzielenia akredytacji dla informacji międzynarodowych jest pisemne potwierdzenie udzielenia akredytacji przez ABW lub SKW określające: zakres akredytacji (akredytowane elementy systemu, klauzule informacji itp.), datę ważności akredytacji, warunki utrzymywania ważności akredytacji.

7. Bezpieczeństwo przemysłowe

1. Bezpieczeństwo przemysłowe – to wszelkie działania związane z zapewnieniem ochrony informacji niejawnych o klauzuli „poufne" lub wyższej, udostępnianych przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej w związku z wykonywaniem przez nich umów lub zadań.
2. Zgodnie z art. 54 ust. 1 uoin warunkiem dopuszczenia przedsiębiorcy do wykonywania umów albo zadań związanych z dostępem do informacji niejawnych, jest jego zdolność do ochrony i zachowania poufności tych informacji[77].
3. Dokumentem potwierdzającym zdolność przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej do zapewnienia ochrony informacji niejawnych jest świadectwo bezpieczeństwa przemysłowego[78] wydane przedsiębiorcy przez ABW albo SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego (art. 54 ust. 2 uoin)[79].

---

[77] Zobowiązanie do zachowania poufności w relacji: zleceniodawca – podmiot wykonujący zlecenie, obliguje wykonawcę do: a) zachowania w tajemnicy wszelkich informacji poufnych, o których dowiedział się z przekazanych mu przez klienta dokumentów, b) niewykorzystywania uzyskanych informacji poufnych w celach innych niż wykonanie pracy, c) zachowania należytej staranności w celu zapewnienia, że osoba trzecia nie uzyska dostępu do dokumentów i materiałów przekazanych przez zleceniodawcę, d) niesporządzania kopii tych materiałów lub dokumentów bez zgody ich właściciela, e) zwrotu, na żądanie klienta, wszystkich dokumentów i materiałów, które otrzymał w celu wykonania umowy (zlecenia). K. Liderman, *Analiza ryzyka i ochrona informacji...*, s. 20.

[78] Wzór świadectwa bezpieczeństwa przemysłowego stanowi załącznik nr 2 do Rozporządzenia w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego. W przypadku gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone" posiadanie świadectwa nie obowiązuje (art. 54 ust. 9 rozp.). Przedsiębiorca ten jest jednak obowiązany spełnić wymagania ustawy w zakresie ochrony informacji niejawnych o klauzuli „zastrzeżone" (uzyskać pisemne upoważnienie kierownika jednostki organizacyjnej, jeżeli nie posiada poświadczenia bezpieczeństwa, oraz odbyć szkolenie w zakresie ochrony informacji niejawnych).

[79] Postępowanie bezpieczeństwa przemysłowego polega na sprawdzeniu danych przedsiębiorcy w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, i obejmuje: a) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła

4. Postępowanie bezpieczeństwa przemysłowego jest prowadzone na wniosek przedsiębiorcy na podstawie wypełnionego kwestionariuszu bezpieczeństwa przemysłowego oraz ankiet lub kopii poświadczeń bezpieczeństwa:
   – kierownika przedsiębiorcy;
   – pełnomocnika ochrony i jego zastępcy;
   – osób zatrudnionych w pionie ochrony;
   – administratora systemu teleinformatycznego;
   – innych osób wskazanych w kwestionariuszu, które powinny mieć dostęp do informacji niejawnych (art. 57 ust. 3 uoin)[80].
5. Postępowanie bezpieczeństwa przemysłowego jest odpłatne i powinno być zakończone w terminie nie dłuższym niż 6 miesięcy, licząc od dnia przedłożenia wszystkich niezbędnych do jego przeprowadzenia dokumentów (art. 59 i 61 uoin).
6. Postępowanie bezpieczeństwa przemysłowego kończy się:
   – wydaniem przez ABW albo SKW świadectwa bezpieczeństwa przemysłowego;
   – odmową wydania świadectwa, stwierdzeniem braku zdolności do ochrony informacji niejawnych[81].
7. W zależności od stopnia zdolności do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej wydaje się świadectwo odpowiednio (art. 55 ust. 1 uoin):
   • pierwszego stopnia – potwierdzające pełną zdolność przedsiębiorcy do ochrony tych informacji;
   • drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych;

---

pochodzenia środków finansowych i sytuację budżetową, b) strukturę organizacyjna przedsiębiorstwa, c) system ochrony informacji niejawnych w przedsiębiorstwie, w tym środki bezpieczeństwa fizycznego, d) wszystkie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia, e) w szczególnie uzasadnionych przypadkach osoby posiadające poświadczenia bezpieczeństwa (art. 57 ust. 1 uoin).

80 Wzór i treść kwestionariusza zawiera załącznik nr 1 do Rozporządzenia w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego.

81 Przesłankami odmowy wydania świadectwa bezpieczeństwa przemysłowego są: a) odmowa wydania lub cofniecie poświadczenia bezpieczeństwa osobie lub osobom, które zajmują stanowisko kierownika przedsiębiorcy, b) brak możliwości ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy, c) niezorganizowanie, w ciągu 6 miesięcy od daty wszczęcia postępowania, kompleksowego systemu ochrony informacji niejawnych (w przypadku ubiegania się o świadectwo pierwszego lub drugiego stopnia), d) zatajenie danych w kwestionariuszu lub podania w nim danych nieprawdziwych, f) niepowiadomienie lub podanie nieprawdziwych informacji o zmianach danych zawartych w kwestionariuszu, g) ujawnienie występowania u osób sprawdzanych niedających się usunąć wątpliwości co do rękojmi zachowania przez nie tajemnicy (art. 64 ust. 2 i 3 uoin).

- trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.

8. Świadectwo potwierdzające zdolność przedsiębiorcy do ochrony informacji niejawnych o klauzuli:
   - „ściśle tajne" potwierdza zdolność do ochrony informacji niejawnych o klauzuli:
     - „ściśle tajne" – przez okres 5 lat od daty wystawienia;
     - „tajne" – przez okres 7 lat od daty wystawienia;
     - „poufne" – przez okres 10 lat od daty wystawienia;
   - „tajne" potwierdza zdolność do ochrony informacji niejawnych o klauzuli:
     - „tajne" – przez okres 7 lat od daty wystawienia;
     - „poufne" – przez okres 10 lat od daty wystawienia;
   - „poufne" potwierdza zdolność do ochrony informacji niejawnych o tej klauzuli przez okres 10 lat od daty wystawienia[82].
9. ABW albo SKW w okresie ważności świadectwa bezpieczeństwa przemysłowego może przeprowadzić z urzędu (lub kontrolne) sprawdzenie przedsiębiorcy w zakresie elementów zawartych w przypisie 75 w celu ustalenia, czy nie utracił on zdolności do ochrony informacji niejawnych (art. 65 ust. 1 i 2 uoin).
10. W wypadku cofnięcia świadectwa bezpieczeństwa przemysłowego ABW albo SKW zawiadamia niezwłocznie jednostki organizacyjne, które zawarły umowy z przedsiębiorcą (art. 66 ust. 4 uoin)[83].
11. W czasie trwania postępowania bezpieczeństwa przemysłowego, a także w okresie ważności świadectwa, przedsiębiorca ma obowiązek informowania odpowiednio ABW albo SKW o:
    - zmianach danych zawartych w kwestionariuszu, w tym nazwy i adresu przedsiębiorcy lub przedmiotu umowy;
    - zawarciu umowy związanej z dostępem do informacji o innej, wyższej klauzuli tajności;
    - ogłoszeniu upadłości, likwidacji jednostki organizacyjnej albo innej formie zakończenia działalności;
    - wypowiedzeniu umowy oraz zakończeniu jej wykonywania (art. 70 ust. 1, 2 i 3 oraz art. 71 ust. 5 uoin).

---

[82] Art. 55 ust. 2 uoin.

[83] Wzór decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego stanowi załącznik nr 3 Rozporządzenia w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, a wzór decyzji cofnięcia – załącznik nr 4. Od decyzji o odmowie wydania oraz cofnięciu świadectwa przedsiębiorcy przysługuje odwołanie do prezesa Rady Ministrów, na którego decyzję lub postanowienie przysługuje skarga do sądu administracyjnego (art. 69 ust. 1 uoin).

8. Zasady przechowywania i udostępniania danych oraz akt postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego

1. Zgodnie z art. 24 ust. 10 uoin ankieta bezpieczeństwa osobowego stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „poufne" w przypadku poszerzonego postępowania sprawdzającego lub „zastrzeżone" w przypadku zwykłego postępowania sprawdzającego[84].
2. Akta postępowań sprawdzających lub kontrolnych postępowań sprawdzających oraz akta postępowań bezpieczeństwa przemysłowego są udostępniane do wglądu lub przekazywane wyłącznie na pisemne żądanie (art. 72 ust. 1 uoin):
   a) sądowi lub prokuratorowi dla celów postępowania karnego;
   b) służbom i organom uprawnionym do przeprowadzenia poszerzonych postępowań sprawdzających tej samej osoby;
   c) właściwemu organowi w celu przeprowadzenia kontroli prawidłowości postępowania, z wyłączeniem postępowań sprawdzających prowadzonych w AW, CBA, BOR, Policji, SW, SWW, SG i ŻW;
   d) właściwemu organowi w celu rozpatrzenia odwołania lub zażalenia; sądowi administracyjnemu w związku z rozpatrywaniem skargi.
3. ABW i SKW są obowiązane do prowadzenia ewidencji osób:
   a) uprawnionych do dostępu do informacji niejawnych o klauzuli „poufne" i wyższej;
   b) którym odmówiono wydania poświadczenia bezpieczeństwa;
   c) wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, z wyłączeniem osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w AW, CBA, BOR, Policji, SW, SWW, SG oraz ŻW (art. 73 ust. 1 uoin)[85].

---

[84] Ankiecie ani formalnie, ani materialno-technicznie nie nadaje się odpowiedniej klauzuli tajności. W rozumieniu ustawy jest ona dokumentem jawnym, ale chronionym (20-letni okres przechowywania, ograniczony dostęp), tak jakby zawierała informacje niejawne.

[85] Dane z ewidencji, o których mowa, mogą obejmować wyłącznie: imię i nazwisko, numer PESEL, imię ojca, datę i miejsce urodzenia, adres zamieszkania lub pobytu, nazwę jednostki organizacyjnej, określenie dokumentu kończącego procedurę, datę wydania oraz numer. Dane te oraz wykazy prowadzone przez pełnomocnika ochrony są udostępniane – na pisemne żądanie – wyłącznie: sądowi lub prokuratorowi oraz właściwemu organowi w celu przeprowadzenia kontroli prawidłowości postępowania (art. 73 ust. 1, 2 i 3 uoin).

Pytania kontrolne

1. Podaj definicję informacji niejawnych i wymień elementy systemu ochrony informacji niejawnych w RP.
2. Podaj oznaczenia klauzuli tajności (ściśle tajne, tajne, poufne, zastrzeżone) w NATO i UE.
3. Kto może być pełnomocnikiem ochrony i wymień jego zadania?
4. Co jest przedmiotem ustaleń w toku postępowania sprawdzającego?
5. Kogo i co obejmuje postępowanie bezpieczeństwa przemysłowego?

Bibliografia

Anzel M., *Szacowanie ryzyka oraz zarządzanie w świetle nowej ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Przykład metody analizy ryzyka opartej na gotowych macierzach*, Poznań 2011.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2005.

Bezpieczeństwo informacyjne III Rzeczypospolitej, red. A. Żebrowski, Kraków 2000.

Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane, red. M. Kwieciński, Kraków 2010.

Bogusz A., *Kwestionariusz bezpieczeństwa przemysłowego – aspekty praktyczne*, [w:] „Ochrona Mienia i Informacji" 2009, nr 1, s. 10–12.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

Decyzja Nr 17/MON Ministra Obrony Narodowej z 20 stycznia 2012 r. w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej (Dz.Urz.MON z 2012 r. poz. 8).

Encyklopedia popularna PWN, red. A. Karwowski, Warszawa 1982.

Garlicki L., *Komentarz do art. 31 Konstytucji RP*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 3, red. L. Garlicki, Warszawa 2003, s. 23–28.

Hoc S., *Karnoprawna ochrona informacji*, Opole 2009.

Hoc S. *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010.

Hoc S., Zaleśny J., *Ochrona informacji niejawnych w Rzeczypospolitej Polskiej*, [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009, s. 261–281.

Informacje niejawne / Bezpieczeństwo teleinformatyczne (zakładka), www.bip.abw.gov.pl/portal/bip.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze sprost. i z późn. zm.).

Kopaliński W., *Słownik wyrazów obcych*, Warszawa 1980.

Iwaszko B., *Ochrona informacji niejawnych w praktyce*, Wrocław 2012.

Jabłoński M., Radziszewski T., *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, Wrocław 2012.

Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice. Wolność informacji, prawo dostępu do informacji publicznej, ochrona danych osobowych*, Wrocław 2002.

Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 1999.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych zagrożeń i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.

Liderman K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Warszawa 2003.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Ochrona informacji niejawnych – Poradnik praktyczny, Warszawa 2011.

Ochrona informacji niejawnych: teoria i praktyka, red. M. Kubiak, Siedlce 2013.

Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VIII Kongresu, red. M. Gajos, Katowice 2012.

Pańkowska M., *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2004.

Pipkin D., *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, Warszawa 2002.

Polaczek A., *Audyt bezpieczeństwa informacji w praktyce*, Gliwice 2006.

Przegląd. Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informatycznych. W kierunku kultury bezpieczeństwa, OECD, 2003, dostępne na: www.oecd.org.

Rozporządzenie Prezesa Rady Ministrów z 25 sierpnia 2005 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych (Dz.U. z 2005 r. Nr 171, poz. 1432).

Rozporządzenie Prezesa Rady Ministrów z 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U. z 2010 r. Nr 258, poz. 1752).

Rozporządzenie Rady Ministrów z dnia 5 kwietnia 2011 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz.U. z 2011 r. Nr 86, poz. 470).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r. Nr 159, poz. 948).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r. Nr 159, poz. 949).

Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2011 r. Nr 276, poz. 1631).

Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. z 2011 r. Nr 271, poz. 1603).

Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. z 2011 r. Nr 288, poz. 1692).

Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r. poz. 683).

Słownik współczesny języka polskiego, red. B. Dunaj, Warszawa 1998.

Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2011.

Thiem P., *Bezpieczeństwo osobowe w ochronie informacji niejawnych*, Wrocław 2011.

Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (t.j. Dz.U. z 2014 r. poz. 1502 z późn. zm.).

Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24 z późn. zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r. Nr 133 poz. 883 z późn. zm., t.j. Dz.U. z 2015 r. poz. 2135, 2281, Dz.U. z 2016 r. poz. 195).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2013 r. poz. 1422).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228).

Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi, ABW, 2010, dostępne na: www.abw.gov.pl (zakładka: Zadania / Informacje niejawne).

Zagadnienia bezpieczeństwa w systemach informacyjnych, red. Z. Huzar, Z. Mazur, Warszawa 2008.

Zarządzenie nr 45 szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 17 sierpnia 2012 r. w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych.

Zarządzanie bezpieczeństwem informacji, red. J. Łuczak, Poznań 2004.

Zarządzanie bezpieczeństwem informacyjnym, red. A. Nowak, W. Scheffs, Warszawa 2010.

Zarządzanie przepływem i ochroną informacji, red. M. Kwieciński, Kraków 2010.

Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000.

Aneks nr 1[86]

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW
z dnia 7 grudnia 2011 r.
w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne
(Dz.U. z 16 2011 r. Nr 271, poz. 1603)

Na podstawie art. 47 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) tryb i sposób nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów, o których mowa w art. 2 pkt 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanych dalej „materiałami";
2) sposób postępowania nadawców przesyłek zawierających informacje niejawne oraz wymogi, jakie muszą spełniać te przesyłki;
3) sposób postępowania podmiotów, które wykonują zadania przewoźników tych materiałów, z przesyłkami zawierającymi informacje niejawne;
4) sposób dokumentowania przyjmowania przez przewoźników przesyłek oraz ich wydawania adresatom, wraz z załącznikami w postaci wzorów niezbędnych formularzy;
5) warunki ochrony i sposoby zabezpieczenia przesyłek przez przewoźnika oraz warunki, jakie muszą spełniać wykorzystywane przez niego środki transportu i uczestniczące w konwojach osoby;
6) sposób postępowania w przypadku zaistnienia nieprzewidzianych okoliczności, mogących mieć wpływ na bezpieczeństwo przesyłki;
7) warunki przewożenia materiałów poza granicami Rzeczypospolitej Polskiej.

§ 2.1. Czynności, o których mowa w § 1 pkt 1, na zlecenie jednostek organizacyjnych wymienionych w art. 1 ust. 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanych dalej „nadawcami", mogą wykonywać następujące podmioty, zwane dalej „przewoźnikami":

1) poczta specjalna podlegająca ministrowi właściwemu do spraw wewnętrznych, działająca w jednostkach organizacyjnych Policji, zapewniająca przewóz materiałów na terytorium Rzeczypospolitej Polskiej;
2) komórka organizacyjna urzędu obsługującego ministra właściwego do spraw zagranicznych, zapewniająca przewóz materiałów za granicę i poza granicami Rzeczypospolitej Polskiej pomiędzy urzędem obsługującym ministra właściwego do spraw zagranicznych i jednostkami organizacyjnymi podległymi lub nadzorowanymi przez tego ministra, zwanymi dalej „placówkami zagranicznymi";
3) właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub Szefowi Kontrwywiadu Wojskowego;

[86] Interpunkcja w tekście zgodna z oryginałem.

4) przedsiębiorcy uprawnieni do wykonywania działalności pocztowej, zwani dalej „operatorami pocztowymi";
5) przedsiębiorcy uprawnieni do wykonywania działalności w zakresie ochrony osób i mienia;
6) przedsiębiorcy uprawnieni do wykonywania działalności w zakresie usług transportowych.

2. Przewoźnik wykonujący czynności, o których mowa w § 1 pkt 1, musi spełniać wymagania w zakresie ochrony informacji niejawnych.

§ 3.1. Materiał o klauzuli „ściśle tajne" lub „tajne" jest przewożony przez przewoźnika, o którym mowa w § 2 ust. 1 pkt 1–3.

2. W szczególnie uzasadnionych przypadkach kierownik jednostki organizacyjnej może zlecić przewiezienie materiału o klauzuli „ściśle tajne" lub „tajne" przewoźnikowi, o którym mowa w § 2 ust. 1 pkt 4 i 5.

§ 4. Materiał o klauzuli „ściśle tajne" lub „tajne" o znacznych rozmiarach lub stanowiący towar niebezpieczny, którego przewóz nie może być zrealizowany przez przewoźnika, o którym mowa w § 2 ust. 1 pkt 1–5, może być przewożony przez przewoźnika, o którym mowa w § 2 ust. 1 pkt 6.

§ 5. Materiał może być przekazywany także bez pośrednictwa przewoźnika, jeżeli jest zabezpieczony przed zniszczeniem oraz dostępem osób nieuprawnionych, a przewóz dokonywany jest przez nadawcę lub adresata, zgodnie z § 8 ust. 1–3 oraz § 12.

§ 6. Nadawca przekazuje przewoźnikowi materiał w postaci przesyłki listowej lub paczki, zwanej dalej „przesyłką", zaadresowanej, zabezpieczonej, opakowanej i oznaczonej zgodnie z wymaganiami określonymi w § 8.

§ 7.1. Przewoźnik przyjmuje przesyłkę na podstawie wykazu przesyłek nadanych, sporządzonego przez nadawcę albo na podstawie dokumentów stosowanych przez operatora pocztowego.

2. Wykaz przesyłek nadanych sporządzany jest w dwóch egzemplarzach, po jednym egzemplarzu dla nadawcy przesyłki i przewoźnika, według wzoru określonego w przepisach wydanych na podstawie art. 47 ust. 1 pkt 11 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą".

3. Przyjęcie przesyłek od nadawcy przewoźnik potwierdza podpisem, zapisami liczbowym i słownym liczby przyjętych przesyłek oraz odciskiem pieczęci na obu egzemplarzach wykazu przesyłek nadanych.

4. W przypadku odmowy przyjęcia przesyłki przez przewoźnika wykreśla się ją na obu egzemplarzach wykazu przesyłek nadanych, potwierdzając to podpisem osoby odmawiającej przyjęcia przesyłki i odciskiem pieczęci przewoźnika.

§ 8.1. Materiał nadawany za pośrednictwem przewoźnika jako przesyłka listowa opakowuje się w dwie nieprzezroczyste koperty, przy czym zamieszcza się:

1) na kopercie wewnętrznej:
   a) klauzulę tajności i ewentualne dodatkowe oznaczenia,
   b) określenie adresata,
   c) imię, nazwisko i podpis osoby pakującej,
   d) numer, pod którym dokument został zarejestrowany;
2) na kopercie zewnętrznej:
   a) nazwę jednostki organizacyjnej adresata,
   b) adres siedziby adresata,
   c) numer wykazu i pozycji w wykazie przesyłek nadanych,
   d) nazwę jednostki organizacyjnej nadawcy.

2. Kopertę wewnętrzną zabezpiecza się w sposób umożliwiający wykrycie prób lub faktu nieuprawnionego dostępu do zawartości.

3. Materiał nadawany za pośrednictwem przewoźnika w postaci paczki opakowuje się w dwie nieprzezroczyste warstwy papieru, oznaczone i zabezpieczone jak w ust. 1 i 2.

4. Materiał przekazywany przez przewoźnika, o którym mowa w § 2 ust. 1 pkt 4, przekazuje się jako przesyłkę poleconą ze zwrotnym potwierdzeniem odbioru.

§ 9. Przesyłki przewozi się w zamkniętej paczce, worku lub innego rodzaju pojemniku, zwanych dalej „pojemnikiem", na którym zamieszcza się pouczenie o postępowaniu w przypadku jego znalezienia.

§ 10.1. Nadawca przed przekazaniem do przewozu przesyłki zawierającej materiał, którego rozmiary lub charakter wymagają zastosowania szczególnych sposobów lub środków ochrony, innych niż te, o których mowa w § 8 i 9, uzgadnia z przewoźnikiem sposoby i środki zabezpieczenia przesyłki przed nieuprawnionym dostępem lub utratą.

2. Uzgodnienia sposobów i środków, o których mowa w ust. 1, dokonuje się, uwzględniając:

1) rozmiary przesyłki;
2) charakterystykę fizyczną i chemiczną, od których zależy bezpieczeństwo przesyłki lub zagrożenie powodowane przez jej przewóz;
3) odpowiednie opakowanie uniemożliwiające identyfikację przewożonego materiału;
4) zapewnienie stałej, o ile to możliwe, łączności między przewoźnikiem i nadawcą.

3. O przewozie przesyłki, o której mowa w ust. 1, zawierającej materiał o klauzuli „ściśle tajne" lub „tajne", nadawca zawiadamia Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW", albo Służbę Kontrwywiadu Wojskowego, zwaną dalej „SKW", wskazując przewoźnika, czas i trasę przewozu.

§ 11.1. Przesyłkę za pośrednictwem przewoźnika przewozi się:
1) środkami publicznego transportu lądowego, przy zapewnieniu wydzielonego miejsca uniemożliwiającego dostęp osób nieuprawnionych do przesyłki lub wydzielenia miejsc gwarantujących ciągły dozór nad przesyłką przez osoby przewożące lub ochraniające, wyposażone w środki łączności oraz broń palną w przypadkach określonych w rozporządzeniu, zwane dalej „konwojentami";
2) samochodami przewoźnika, w sposób uniemożliwiający dostęp osób nieuprawnionych do przesyłki, przy zapewnieniu ciągłego dozoru nad przesyłką przez konwojentów;
3) statkami powietrznymi lub środkami transportu wodnego, przy zapewnieniu wydzielonego miejsca uniemożliwiającego dostęp osób nieuprawnionych do przesyłki lub wydzielenia miejsc gwarantujących ciągły dozór nad przesyłką przez konwojentów.

2. Przewóz przesyłki bez pośrednictwa przewoźnika odbywa się pod warunkiem zabezpieczenia przesyłki przed dostępem osób nieuprawnionych.

§ 12.1. Przesyłkę zawierającą informacje niejawne o klauzuli „ściśle tajne" przewozi i ochrania konwój złożony co najmniej z dwóch uzbrojonych w broń palną konwojentów posiadających odpowiednie poświadczenia bezpieczeństwa.

2. Przesyłkę zawierającą informacje niejawne o klauzuli „tajne" przewozi i ochrania co najmniej jeden uzbrojony w broń palną konwojent posiadający odpowiednie poświadczenie bezpieczeństwa.

3. Przesyłkę zawierającą informacje niejawne o klauzuli „poufne" lub „zastrzeżone" przewozi i ochrania co najmniej jeden konwojent posiadający odpowiednie poświadczenie bezpieczeństwa lub upoważnienie.

4. Wymóg posiadania broni palnej nie dotyczy przesyłek przewożonych za granicę i poza granicami Rzeczypospolitej Polskiej, a także przypadków, gdy przesyłka jest przekazywana bez pośrednictwa przewoźnika od nadawcy do adresata lub na terenie tej samej miejscowości.

5. Konwojentów wyposaża się w środki łączności umożliwiające kontakt z nimi podczas przewozu oraz zapoznaje się z zasadami postępowania z ochranianymi i przewożonymi przesyłkami.

§ 13. Materiał o klauzuli „ściśle tajne" lub „tajne" nie może być przewożony łącznie z przedmiotami niebezpiecznymi lub stwarzającymi znaczne zagrożenie ich kradzieży bądź uszkodzenia.

§ 14. Przewóz przesyłki planuje się w taki sposób, aby została dostarczona w możliwie najkrótszym czasie do adresata.

§ 15.1. W czasie załadunku, przewożenia, przeładunku i wyładunku przesyłki niedopuszczalne jest pozostawienie jej bez nadzoru konwojentów.

2. Przesyłka czasowo przechowywana poza środkiem transportu powinna znajdować się w zamkniętym, chronionym miejscu, do którego dostęp mogą mieć tylko osoby posiadające odpowiednie poświadczenie bezpieczeństwa lub inne uprawnienie do dostępu do informacji niejawnych.

3. Każdy fakt przechowywania, o którym mowa w ust. 2, odnotowuje się w wykazie przesyłek nadanych, w rubryce „Uwagi".

§ 16.1. W przypadku uszkodzenia przesyłki lub stwierdzenia śladów jej otwierania przewoźnik zabezpiecza ją w celu niedopuszczenia do dalszych uszkodzeń i ujawnienia jej zawartości oraz sporządza protokół w sprawie uszkodzenia przesyłki w trzech egzemplarzach, z których pierwszy wydaje się adresatowi, drugi wysyła się do nadawcy, a trzeci pozostaje u przewoźnika.

2. Przesyłkę, o której mowa w ust. 1, wraz ze sporządzonym protokołem w sprawie uszkodzenia przesyłki wydaje się adresatowi.

3. W przypadku odmowy przyjęcia przez adresata uszkodzonej przesyłki przewoźnik zwraca ją nadawcy wraz z protokołem, o którym mowa w ust. 1, i naniesioną na nim adnotacją o przyczynie odmowy przyjęcia przesyłki.

4. Przepisy ust. 1–3 stosuje się odpowiednio w przypadkach, gdy mogło dojść do ujawnienia lub doszło do ujawnienia treści przesyłki, załączając do protokołu wyjaśnienia, komu i w jakich okolicznościach jej treść mogła zostać lub została ujawniona.

5. Wzór protokołu w sprawie uszkodzenia przesyłki stanowi załącznik nr 1 do rozporządzenia.

§ 17.1. Przewoźnik wydaje przesyłkę upoważnionemu przedstawicielowi adresata na podstawie wykazu przesyłek wydanych, sporządzonego przez przewoźnika.

2. Wzór wykazu przesyłek wydanych stanowi załącznik nr 2 do rozporządzenia.

3. Przed odebraniem przesyłki przedstawiciel adresata jest obowiązany przedstawić upoważnienie do jej odbioru.

4. Wzór upoważnienia do nadawania i odbioru przesyłek stanowi załącznik nr 3 do rozporządzenia.

5. W przypadku przekazania przesyłki bez pośrednictwa przewoźnika upoważniony przedstawiciel adresata potwierdza pisemnie nadawcy jej odbiór.

6. Pracownik jednostki organizacyjnej adresata uprawniony do odbioru przesyłki niezwłocznie przekazuje ją do kancelarii tajnej lub komórki organizacyjnej, w której rejestrowane są materiały. Przepisy § 18 ust. 1–3 stosuje się odpowiednio.

§ 18.1. Kierownik kancelarii tajnej lub inny upoważniony pracownik komórki organizacyjnej, w której rejestrowane są materiały, przyjmuje przesyłkę za pokwitowaniem i odciska na niej pieczęć oraz datę wpływu do jednostki organizacyjnej.

2. Przyjmując przesyłkę, sprawdza się:
1) prawidłowość oznaczenia nadawcy i adresata;
2) całość pieczęci i opakowania;
3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy.

3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania osoba kwitująca odbiór przesyłki sporządza, wraz z doręczającym, protokół w sprawie uszkodzenia, o ile protokół nie został sporządzony przez przewoźnika w trybie, o którym mowa w § 16 ust. 1. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi – pełnomocnikowi do spraw ochrony informacji niejawnych w jednostce organizacyjnej adresata, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także przewoźnikowi.

4. Kierownik kancelarii tajnej lub inny upoważniony pracownik komórki organizacyjnej, w której rejestrowane są materiały, odnotowuje fakt sporządzenia protokołu, o którym mowa w ust. 3, w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi".

§ 19.1. Przesyłkę, o której adresat został powiadomiony przez przewoźnika, uznaje się za nieodebraną po 7 dniach od daty zawiadomienia i odsyła do nadawcy.

2. Terminu, o którym mowa w ust. 1, nie stosuje się w przypadku przewoźnika, o którym mowa w § 2 ust. 1 pkt 2.

§ 20.1. W przypadku powzięcia przez nadawcę informacji o niedostarczeniu przez przewoźnika przesyłki nadawca występuje do przewoźnika z żądaniem podjęcia czynności wyjaśniających. Jeżeli czynności potwierdzą utratę przesyłki, przewoźnik ustala osoby odpowiedzialne za utratę przesyłki oraz okoliczności, w jakich utrata przesyłki nastąpiła. W przypadku utraty materiału o klauzuli „poufne" lub wyższej nadawca informuje o tym fakcie ABW albo SKW.

2. Przewoźnik po dokonaniu ustaleń, o których mowa w ust. 1, udziela nadawcy odpowiedzi na piśmie, nie później niż w terminie 2 tygodni od otrzymania od nadawcy informacji o utracie przesyłki, a w przypadku utraty materiału o klauzuli „poufne" lub wyższej informuje równocześnie ABW albo SKW o dokonanych ustaleniach.

§ 21.1. W przypadku zaistnienia nieprzewidzianych okoliczności, mogących mieć wpływ na bezpieczeństwo przesyłki, przewoźnik podejmuje odpowiednie do okoliczności działania zmierzające do ochrony przesyłki oraz niezwłocznie zawiadamia nadawcę i adresata o zdarzeniu.

2. W przypadku gdy zdarzenie, o którym mowa w ust. 1, dotyczy przesyłki zawierającej informacje niejawne o klauzuli „ściśle tajne" lub „tajne", przewoźnik dodatkowo zawiadamia ABW albo SKW.

§ 22.1. Jeżeli zawarte umowy międzynarodowe nie stanowią inaczej, materiał przekazuje się za granicę i poza granicami Rzeczypospolitej Polskiej za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 2 lub 3. Przepis § 4 stosuje się odpowiednio.

2. Materiał o klauzuli „zastrzeżone" może być przesyłany za granicę oraz poza granicami Rzeczypospolitej Polskiej także za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 4, z uwzględnieniem zasad zabezpieczenia i pakowania określonych w § 8.

3. Materiał określony w § 4 może być przekazywany poza granice Rzeczypospolitej Polskiej za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 6, z uwzględnieniem zasad zabezpieczenia i pakowania określonych w § 9.

4. Na każdym pojemniku przewożonym przez przewoźnika, o którym mowa w § 2 ust. 1 pkt 2, umieszcza się dane o nadawcy i adresacie oraz odciski pieczęci urzędowej.

5. Przewoźnik, o którym mowa w § 2 ust. 1 pkt 2, wydaje upoważnionemu przedstawicielowi adresata pojemnik z przesyłkami na podstawie listu kurierskiego.

6. Przesyłki przewożone przez przewoźnika, o którym mowa w § 2 ust. 1 pkt 2, w przypadku gdy ich adresatami są akredytowani przedstawiciele innych jednostek organizacyjnych niż urząd obsługujący ministra właściwego do spraw zagranicznych, mogą być przekazane przez konwojentów bezpośrednio do adresata, o ile posiada on warunki do ich bezpiecznego przechowywania określone w ustawie.

7. Przesyłki, których nadawcami są akredytowani przedstawiciele innych jednostek organizacyjnych niż urząd obsługujący ministra właściwego do spraw zagranicznych, mogą być przekazane bezpośrednio konwojentom przewoźnika, o którym mowa w § 2 ust. 1 pkt 2.

§ 23.1. W przypadku gdy zachodzi konieczność pilnego wywozu poza granicę Rzeczypospolitej Polskiej materiału i nie istnieje możliwość przekazania materiału za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 2–4, kierownik jednostki delegującej może zezwolić na wywóz tego materiału, jeżeli osoba wywożąca:

1) posiada odpowiednie poświadczenie bezpieczeństwa lub upoważnienie;
2) zapewnia stałą osobistą ochronę i bezpośredni nadzór w czasie podróży nad przewożonym materiałem;
3) ma zapewniony środek transportu umożliwiający bezpieczny przewóz materiału do miejsca, w którym materiał będzie wykorzystywany;
4) posiada środek łączności umożliwiający szybki kontakt z jednostką delegującą;
5) ma zapewnione miejsce gwarantujące bezpieczne przechowywanie tego materiału;
6) posiada paszport dyplomatyczny.

2. Przed wydaniem zezwolenia, o którym mowa w ust. 1, kierownik jednostki delegującej, z wyjątkiem służb, o których mowa wart. 23 ust. 5 ustawy, jest obowiązany powiadomić ABW albo SKW o potrzebie wywozu materiału o klauzuli „ściśle tajne" lub „tajne".

3. Zdeponowanie materiału w placówce zagranicznej uzgadnia się z urzędem obsługującym ministra właściwego do spraw zagranicznych.

4. Osobie wywożącej materiał za granicę wydaje się list kurierski oraz zapoznaje się ją z zasadami postępowania z tym materiałem.

5. Wymogów, o których mowa w ust. 1 pkt 6 i ust. 4, nie stosuje się:

1) w przypadku przewożenia materiału o klauzuli „zastrzeżone";
2) w przypadku przewożenia materiału o klauzuli „poufne" przez terytorium państw członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego.

6. Do przywozu z zagranicy oraz do przewozu poza granicami Rzeczypospolitej Polskiej materiałów przepisy ust. 1–4 stosuje się odpowiednio.

§ 24. Rozporządzenie wchodzi w życie z dniem 1 stycznia 2012 r.

Prezes Rady Ministrów: D. Tusk

Aneks nr 2[87]

ROZPORZĄDZENIE RADY MINISTRÓW
z dnia 7 grudnia 2011 r.
w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych
(Dz.U. z 2011 r Nr 276, poz. 1631)

Na podstawie art. 47 ust. 1 pkt 2 i 7–11 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228) zarządza się, co następuje:

§ 1.1. Rozporządzenie określa:
1) wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych;
2) strukturę organizacyjną kancelarii, z uwzględnieniem możliwości tworzenia jej oddziałów;
3) podstawowe zadania kierownika kancelarii;
4) sposób i tryb przetwarzania informacji niejawnych;
5) wzór karty zapoznania się z dokumentem;
6) wzory dzienników ewidencji.

2. Przepisów rozporządzenia regulujących sprawy, o których mowa w ust. 1 pkt 1–4, nie stosuje się w jednostkach organizacyjnych organów wymienionych w art. 47 ust. 3 i 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą", oraz w stosunku do informacji niejawnych wchodzących w skład zasobu archiwalnego archiwów państwowych.

§ 2.1. Tworząc kancelarię tajną, o której mowa w art. 42 ust. 1 ustawy, zwaną dalej „kancelarią", zapewnia się spełnienie następujących wymagań w zakresie organizacji i funkcjonowania:
1) wyodrębnienie organizacyjne i lokalizacyjne;
2) sprawne i bezpieczne rejestrowanie, przechowywanie, obieg i wydawanie materiałów, o których mowa w art. 2 pkt 4 ustawy, zwanych dalej „materiałami", umożliwiające w każdej chwili ustalenie, gdzie znajduje się zarejestrowany materiał oraz kto i kiedy się z tym materiałem zapoznał;
3) właściwą strukturę organizacyjną uwzględniającą następujące elementy:
   a) kancelarią kieruje kierownik kancelarii,
   b) oddziałem kancelarii kieruje osoba wyznaczona przez pełnomocnika ochrony spośród pracowników pionu ochrony.

2. W celu realizacji wymogów, o których mowa w ust 1 pkt 2, prowadzi się następujące dzienniki ewidencji:
1) rejestr dzienników ewidencji i teczek, którego wzór stanowi załącznik nr 1 do rozporządzenia;

[87] Interpunkcja w tekście zgodna z oryginałem.

2) dziennik ewidencyjny, którego wzór stanowi załącznik nr 2 do rozporządzenia;
3) książkę doręczeń przesyłek miejscowych, której wzór stanowi załącznik nr 4 do rozporządzenia;
4) wykaz przesyłek nadanych, którego wzór stanowi załącznik nr 5 do rozporządzenia;
5) rejestr wydanych przedmiotów służący do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów, którego wzór stanowi załącznik nr 6 do rozporządzenia.

3. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych w kancelarii:
1) można prowadzić także inne dzienniki ewidencji niż wymienione w ust. 2;
2) można tworzyć oddziały funkcjonujące w sposób określony dla kancelarii.

4. W pomieszczeniach kancelarii można wydzielić miejsce, w którym osoby uprawnione mogą zapoznawać się z materiałami, zwane dalej „czytelnią", spełniające następujące wymagania:
1) czytelnię organizuje się w sposób umożliwiający stały nadzór pracowników kancelarii nad materiałami;
2) w czytelni zabrania się instalowania systemu monitoringu wizyjnego.

5. Przepisy ust. 2 i 3 stosuje się odpowiednio do organizacji pracy innych niż kancelaria tajna komórek organizacyjnych, o których mowa w art. 44 ust. 1 ustawy.

§ 3.1. Dzienniki ewidencji można prowadzić w formie elektronicznego rejestru.

2. W przypadku przetwarzania w dzienniku ewidencji, o którym mowa w ust. 1, wyłącznie informacji jawnych zapewnia się spełnienie wymagań określonych w przepisach wydanych na podstawie art. 18 ustawy *z* dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565, z późn. zm.).

§ 4.1. Do podstawowych zadań kierownika kancelarii, w odniesieniu do materiałów podlegających rejestracji w kancelarii, należy:
1) bezpośredni nadzór nad obiegiem materiałów;
2) udostępnianie materiałów osobom do tego uprawnionym;
3) wydawanie materiałów osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania;
4) egzekwowanie zwrotu materiałów;
5) kontrola przestrzegania właściwego oznaczania i rejestrowania materiałów w kancelarii oraz jednostce organizacyjnej;
6) nadzór nad pracą oddziałów kancelarii.

2. Osoba kierująca oddziałem kancelarii wykonuje obowiązki kierownika kancelarii określone w ust. 1 pkt 1–5.

§ 5.1. W przypadku zmiany na stanowisku kierownika kancelarii lub osoby kierującej oddziałem kancelarii sporządza się protokół zdawczo-odbiorczy.

2. Protokół, o którym mowa w ust. 1, sporządza się w obecności osoby zdającej obowiązki, osoby przejmującej obowiązki oraz pełnomocnika ochrony lub upoważnionej przez niego osoby. Protokół sporządza się w dwóch egzemplarzach; pierwszy egzemplarz przechowuje się w kancelarii, drugi przechowuje pełnomocnik ochrony.

3. W przypadku czasowej nieobecności kierownika kancelarii lub osoby kierującej oddziałem kancelarii ich obowiązki przejmuje pełnomocnik ochrony lub pracownik kancelarii pisemnie przez niego upoważniony.

§ 6.1. Po zakończeniu pracy kierownik kancelarii lub inny upoważniony pracownik jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń kancelarii.

2. Wszelkie przypadki naruszenia zasad ochrony informacji niejawnych należy niezwłocznie zgłaszać pełnomocnikowi ochrony.

§ 7.1. Kierownik kancelarii lub inny upoważniony pracownik niezwłocznie rejestruje przyjęte materiały w odpowiednim dzienniku lub rejestrze.

2. W przypadku każdego dokumentu o klauzuli „ściśle tajne" lub „tajne" z chwilą jego udostępnienia zakłada się kartę zapoznania się z dokumentem, którą dołącza się do dokumentu. Wzór karty zapoznania się z dokumentem stanowi załącznik nr 3 do rozporządzenia.

3. W przypadku zbioru dokumentów zakłada się jedną kartę zapoznania się z dokumentem. Kartę zapoznania się z dokumentem pozostawia się w jednostce organizacyjnej, w której została założona, i przechowuje się tak długo, jak dziennik ewidencyjny, w którym dokument został zarejestrowany.

4. Kierownik kancelarii lub inny upoważniony pracownik przekazuje albo udostępnia zarejestrowane materiały adresatowi lub upoważnionej przez adresata osobie, za pokwitowaniem.

5. Po otwarciu przesyłki kierownik kancelarii tajnej lub inny upoważniony pracownik komórki organizacyjnej, w której rejestrowane są materiały:

1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
2) ustala, czy liczba stron lub innych jednostek miary materiałów oraz liczba załączników jest zgodna z liczbą oznaczoną na poszczególnych materiałach.

6. W przypadku stwierdzenia nieprawidłowości w wyniku czynności, o których mowa w ust. 5, kierownik kancelarii tajnej lub inny upoważniony pracownik komórki organizacyjnej, w której rejestrowane są materiały, sporządza protokół z otwarcia przesyłki, zawierający opis nieprawidłowości, w dwóch egzemplarzach, z których jeden przekazuje się do nadawcy, a drugi pozostawia u adresata.

7. Kierownik kancelarii tajnej lub inny upoważniony pracownik komórki organizacyjnej, w której rejestrowane są materiały, odnotowuje fakt sporządzenia

protokołu, o którym mowa w ust. 6, w odpowiednim urządzeniu ewidencyjnym w rubryce „Informacje uzupełniające/Uwagi".

§ 8.1. W kancelarii nie otwiera się przesyłek oznaczonych „do rąk własnych". W odpowiednim dzienniku lub rejestrze wpisuje się nadawcę, numer i datę wpływu przesyłki; w rubryce „Informacje uzupełniające/Uwagi" odnotowuje się, że przesyłka była oznaczona „do rąk własnych".

2. Na opakowaniu przesyłek, o których mowa w ust. 1, wpisuje się datę wpływu i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się, za pokwitowaniem, bezpośrednio adresatowi, a w razie jego nieobecności – osobie przez niego pisemnie upoważnionej do odbioru.

3. Po otwarciu przesyłki, o której mowa w ust. 1, odbiorca przesyłki:

1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
2) ustala, czy liczba stron lub innych jednostek miary materiałów oraz liczba załączników jest zgodna z liczbą oznaczoną na poszczególnych materiałach.

4. Z chwilą zwrotu do kancelarii przesyłki, o której mowa w ust. 1, kierownik kancelarii lub inny upoważniony pracownik uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.

5. Jeżeli adresat podjął decyzję o przechowywaniu w kancelarii przesyłki oznaczonej „do rąk własnych" w stanie zamkniętym, kierownik kancelarii lub inny upoważniony pracownik dokonuje czynności, o których mowa w ust. 4, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

§ 9.1. Otrzymaną albo wysyłaną przesyłkę bądź wytworzony dokument lub inny materiał rejestruje się w dzienniku ewidencji odpowiednio w kolejności otrzymania, wysłania lub wytworzenia.

2. Rejestracji, o których mowa w ust. 1, dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym. Zmian w dzienniku ewidencji dokonuje się kolorem czerwonym, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej zmiany.

3. W przypadku anulowania pozycji w dzienniku ewidencji podaje się powód anulowania, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej anulowania. Anulowania pozycji w dzienniku ewidencji dokonuje się kolorem czerwonym.

4. Zabrania się wycierania, zamazywania lub nadpisywania zapisów dokonanych w dziennikach ewidencji.

5. W elektronicznych rejestrach dokumentów nie usuwa się zapisów ani nie dokonuje się zmian, o których mowa w ust. 2–4. W rejestrach tych zamieszcza się informacje o zmianach i skreśleniach.

§ 10.1. Dokument, który nie jest przewidziany do dalszego wykorzystywania, o ile nie stanowi materiału archiwalnego, może zostać zniszczony, z zastrzeżeniem przepisów o narodowym zasobie archiwalnym i archiwach.

2. Dokument niszczy się w taki sposób, aby niemożliwe było całkowite lub częściowe odtworzenie jego treści.

3. Po protokolarnym zniszczeniu dokumentu uzupełnia się rejestry, dzienniki i inne informacje dotyczące jego rejestracji.

§ 11. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne międzynarodowe, tworząc kancelarię tajną międzynarodową, uwzględnia przepisy, których Rzeczpospolita Polska jest zobowiązana przestrzegać na mocy zawartych umów międzynarodowych.

§ 12. Formularze dzienników, rejestrów oraz innych urządzeń ewidencyjnych stosowane według dotychczasowych wzorów mogą być wykorzystywane do wyczerpania zapasów, nie dłużej jednak niż do dnia 31 grudnia 2013 r.

§ 13. Rozporządzenie wchodzi w życie z dniem 1 stycznia 2012 r.

Prezes Rady Ministrów: D. Tusk

Aneks nr 3[88]

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW
z dnia 22 grudnia 2011 r.
w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności
(Dz.U. z 2011 r. Nr 288, poz. 1692)

Na podstawie art. 6 ust. 9 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228) zarządza się, co następuje:

§ 1. Rozporządzenie określa sposób oznaczania materiałów, o których mowa w art. 2 pkt 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanych dalej „materiałami", umieszczania na nich klauzul tajności, a także tryb i sposób zmiany lub znoszenia nadanej klauzuli.

§ 2. Ilekroć w rozporządzeniu jest mowa o:
1) oznaczaniu – należy przez to rozumieć czynność techniczną nanoszenia na materiał informacji określonych w rozporządzeniu, w tym umieszczania na nim klauzuli tajności, oraz nanoszenia informacji o zmianie lub zniesieniu nadanej klauzuli, a także umieszczania informacji w metryce dokumentu elektronicznego;
2) informatycznym nośniku danych – należy przez to rozumieć materiał lub urządzenie w rozumieniu art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565, z późn. zm.);
3) dokumencie elektronicznym – należy przez to rozumieć dokument utrwalony na informatycznym nośniku danych lub przetwarzany w systemie teleinformatycznym, o ile ze względu na organizację obiegu informacji niejawnych podlega rejestracji;
4) dokumencie nieelektronicznym – należy przez to rozumieć dokument utrwalony na nośniku innym niż informatyczny nośnik danych, o ile ze względu na organizację obiegu informacji niejawnych podlega rejestracji;
5) metryce dokumentu elektronicznego – należy przez to rozumieć zestaw informacji o dokumencie elektronicznym, powiązanych z dokumentem lub umieszczonych na nim, stanowiących jego oznaczenie w rozumieniu rozporządzenia;
6) odwzorowaniu cyfrowym – należy przez to rozumieć przekształcenie dokumentu nieelektronicznego w dokument elektroniczny dokonywane w szczególności przez jego zeskanowanie;
7) kopiowaniu – należy przez to rozumieć w szczególności również wykonywanie odpisu, wypisu, wyciągu, wydruku, odwzorowania cyfrowego lub nagrania.

[88] Interpunkcja w tekście zgodna z oryginałem.

§ 3.1. Materiał oznacza się klauzulą tajności w sposób wyraźny i w pełnym brzmieniu.

2. W przypadku gdy poszczególnym częściom materiału zostały nadane różne klauzule tajności bądź gdy niektóre z tych części są jawne, wyodrębnione części oddziela się oznaczeniem odpowiedniej klauzuli tajności wskazanej w pełnym brzmieniu lub określeniem „jawne". Części materiału zawierające tekst lub obraz oddziela się przez odpowiednie ich oznaczenie przed rozpoczęciem i po zakończeniu tekstu lub obrazu.

3. Jeżeli poszczególnym częściom materiału zostały nadane różne klauzule tajności, materiał oznacza się klauzulą tajności co najmniej równą najwyższej klauzuli tajności, jaką nadano części materiału.

§ 4. Wprowadza się następujące symbole oznaczenia klauzul tajności:
1) „00" – dla klauzuli „ściśle tajne";
2) „O" – dla klauzuli „tajne";
3) „Pf" – dla klauzuli „poufne";
4) „Z" – dla klauzuli „zastrzeżone".

§ 5.1. Dokument nieelektroniczny utrwalony w formie pisma oznacza się w następujący sposób:
1) na każdej stronie umieszcza się:
   a) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności,
   b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy",
   c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym ten dokument został zarejestrowany, i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca wykonania dokumentu w jednostce lub komórce organizacyjnej lub też jego przynależność do określonej sprawy,
   d) numer strony oraz liczbę stron całego dokumentu,
   e) na środku, jako ostatni element w stopce strony, klauzulę tajności;
2) na pierwszej stronie umieszcza się również:
   a) nazwę jednostki lub komórki organizacyjnej,
   b) nazwę miejscowości i datę podpisania dokumentu,
   c) w przypadku dokumentu, któremu nadano bieg korespondencyjny, imię i nazwisko lub nazwę stanowiska adresata; w przypadku wielu adresatów dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika";
3) na ostatniej stronie pod treścią umieszcza się również:
   a) liczbę załączników,
   b) liczbę stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,

c) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane, oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
d) w przypadku gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat" – jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, lub napis „do zwrotu" – jeżeli załączniki mają zostać zwrócone nadawcy,
e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania,
f) liczbę wykonanych egzemplarzy,
g) adresatów poszczególnych egzemplarzy dokumentu albo adnotację „adresaci według rozdzielnika",
h) dyspozycję „ad acta" w przypadku egzemplarza pozostającego w aktach nadawcy,
i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę.

2. W przypadku dokumentu, o którym mowa w ust. 1, o klauzuli „zastrzeżone" dopuszcza się odstąpienie od umieszczania oznaczeń, o których mowa w ust. 1 pkt 1 lit. b oraz pkt 3 lit. f–i.

§ 6.1. Dokument elektroniczny oznacza się w ten sposób, że jego metryka zawiera następujące informacje:
1) klauzulę tajności;
2) sygnaturę literowo-cyfrową, o której mowa w § 5 ust. 1 pkt 1 lit. c;
3) nazwę jednostki lub komórki organizacyjnej;
4) datę rejestracji dokumentu;
5) w przypadku dokumentu, któremu nadano bieg korespondencyjny, wskazanie adresatów przez podanie imion i nazwisk lub nazw ich stanowisk;
6) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane;
7) stanowisko, imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do podpisania dokumentu;
8) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę;
9) nazwę nadaną dokumentowi lub określenie, czego dokument dotyczy.

2. Pełną nazwę klauzuli tajności nanosi się, o ile to możliwe, na dokumencie elektronicznym.

3. W przypadku dokumentu elektronicznego o klauzuli „zastrzeżone" § 5 ust. 2 stosuje się odpowiednio.

§ 7.1. Na dokumencie nieelektronicznym można zamieścić dyspozycję dotyczącą:
1) braku zgody na kopiowanie lub tłumaczenie części albo całości dokumentu;
2) braku zgody na udzielanie informacji o treści dokumentu;
3) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu.

2. W przypadku dokumentu elektronicznego dyspozycję, o której mowa w ust.1, można zamieścić w jego metryce.

§ 8. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych, na materiałach zawierających informacje niejawne można nanosić w sposób czytelny, widoczny i trwały dodatkowe oznaczenia, inne niż te, o których mowa w § 5–7.

§ 9.1. Na dokumencie nieelektronicznym stanowiącym załącznik na pierwszej stronie umieszcza się dodatkowo informację: „Załącznik nr… do dokumentu nr… z dnia…".

2. Jeżeli wraz z dokumentem przesyła się załączniki zawierające informacje niejawne, to:

1) dokument oznacza się klauzulą tajności nie niższą niż najwyższa klauzula tajności załączników;
2) na dokumencie – jeżeli po trwałym odłączeniu załączników dokument jest jawny albo jego klauzula tajności jest inna niż określona zgodnie z pkt 1 – na każdej stronie pod numerem egzemplarza umieszcza się adnotację o jawności albo klauzuli tajności dokumentu po odłączeniu załączników.

3. W przypadku dokumentu elektronicznego informacje, o których mowa w ust. 1 i 2, umieszcza się odpowiednio w jego metryce.

4. Informację, o której mowa w ust. 1, umieszcza się, w miarę możliwości, na materiałach innych niż dokumenty.

§ 10.1. Na materiałach innych niż dokumenty, o których mowa w § 5 i 6, klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, w szczególności na ich obudowie lub opakowaniu.

2. Materiał, który ze względu na organizację obiegu informacji niejawnych nie podlega rejestracji, oznacza się w sposób zapewniający jednoznaczną identyfikację jego klauzuli tajności, w szczególności przez jej umieszczenie na materiale.

3. Utrwalanie informacji niejawnych w formie dźwięku lub obrazu poprzedza się i kończy informacją o nadanej klauzuli tajności, o ile istnieją takie możliwości.

§ 11. Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach klauzule tajności umieszcza się pośrodku, na górze i na dole zewnętrznych ścianek okładki oraz – jeżeli jest – na stronie tytułowej.

§ 12. Zgody na zniesienie lub zmianę klauzuli tajności udziela się w odrębnym dokumencie podlegającym rejestracji lub przez oznaczenie w postaci umieszczenia informacji:

1) na dokumencie – w przypadku dokumentu nieelektronicznego;
2) w metryce dokumentu – w przypadku dokumentu elektronicznego.

§ 13.1. Oznaczenia zniesienia klauzuli tajności na dokumencie nieelektronicznym utrwalonym w formie pisma dokonuje się następująco:
1) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;
2) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się napis „Zniesiono klauzulę tajności" oraz datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności.

2. Oznaczenia zmiany klauzuli tajności na dokumencie, o którym mowa w ust. 1, dokonuje się następująco:
1) skreśla się wszystkie dotychczasowe oznaczenia klauzuli tajności;
2) nad skreślonymi oznaczeniami klauzul tajności umieszcza się oznaczenie nowej klauzuli tajności;
3) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności.

3. Skreśleń i adnotacji, o których mowa w ust. 1 i 2, dokonują: kierownik kancelarii tajnej, kierownik archiwum lub jego zastępca, kierownik innej niż kancelaria tajna komórki, w której są rejestrowane materiały niejawne, albo inne osoby upoważnione przez nich lub przez kierownika jednostki organizacyjnej.

4. Skreśleń i adnotacji, o których mowa w ust. 1 i 2, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.

5. Oznaczenie zmiany lub zniesienia klauzuli tajności dokumentu elektronicznego umieszcza się w jego metryce. W przypadku, o którym mowa w § 6 ust. 2, oznaczenie umieszcza się, o ile to możliwe, na dokumencie.

§ 14. W przypadku materiałów, o których mowa w § 10 i 11, przepis § 13 stosuje się odpowiednio, z uwzględnieniem sposobu oznakowania tych materiałów.

§ 15.1. Na dokumencie nieelektronicznym wytworzonym w wyniku kopiowania lub tłumaczenia umieszcza się:
1) w przypadku kopii – na pierwszej stronie sygnaturę, o której mowa w § 5 ust. 1 pkt 1 lit. c;
2) w pozostałych przypadkach – odpowiednio oznaczenia, o których mowa w § 5;
3) na wszystkich stronach:
   a) w przypadku kopiowania napis „Wydruk", „Kopia", „Odpis", „Wyciąg" albo „Wypis",

b) w przypadku tłumaczenia napis „Tłumaczenie z języka (nazwa języka)" oraz podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tłumaczenia;

4) na ostatniej stronie w przypadku kopiowania dodatkowo potwierdzenie zgodności z oryginałem zawierające:
   a) napis „Za zgodność",
   b) odcisk pieczęci z nazwą jednostki lub komórki organizacyjnej, w której wytworzono dokument,
   c) podpis, imię i nazwisko lub inne oznaczenie wskazujące kierownika jednostki lub komórki organizacyjnej, w której dokonano kopiowania, albo osobę przez niego upoważnioną.

2. Wytworzenie dokumentu w wyniku kopiowania lub tłumaczenia dokumentu nieelektronicznego odnotowuje się na ostatniej stronie dokumentu kopiowanego lub tłumaczonego przez umieszczenie informacji o:

1) nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument;
2) liczbie egzemplarzy dokumentu wytworzonego;
3) dacie wytworzenia dokumentu;
4) numerze, pod jakim wytworzony dokument został zarejestrowany.

3. Informacje, o których mowa w ust. 2 pkt 1–3, umieszcza się przed wytworzeniem dokumentu w wyniku kopiowania lub tłumaczenia, natomiast numer, pod jakim został on zarejestrowany, umieszcza się po wytworzeniu.

4. W przypadku kopiowania lub tłumaczenia dokumentu elektronicznego informacje, o których mowa w ust. 2 pkt 1–4, umieszcza się w jego metryce.

5. W metryce dokumentu elektronicznego wytworzonego w wyniku kopiowania lub tłumaczenia umieszcza się:

1) informacje, o których mowa w § 6;
2) odpowiednio informację: „Odwzorowanie cyfrowe", „Kopia", „Odpis", „Wyciąg", „Wypis" albo „Tłumaczenie z języka (nazwa języka)";
3) imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą kopiowania albo tłumaczenia.

6. W przypadku dokumentu o klauzuli „zastrzeżone" dopuszcza się odstąpienie od umieszczenia oznaczeń, o których mowa w ust. 1 pkt 3 i 4, ust. 2 i 4 oraz ust. 5 pkt 2 i 3.

7. W przypadku wytwarzania dokumentów w wyniku kopiowania lub tłumaczenia materiałów archiwalnych zgromadzonych w archiwach państwowych albo archiwach wyodrębnionych nie dokonuje się czynności, o których mowa w ust. 2, z tym że do materiałów archiwalnych dołącza się kartę informacyjną, na której każdorazowo umieszcza się informację o wytworzeniu dokumentów w wyniku kopiowania lub tłumaczenia, z uwzględnieniem informacji, o których mowa w ust. 2.

§ 16. Materiały zawierające informacje niejawne wykorzystywane w urządzeniach lub systemach przeznaczonych do wykonywania czynności operacyj-

no-rozpoznawczych, w szczególności urządzenia, części urządzeń lub informatyczne nośniki danych, nie podlegają oznaczeniu w sposób określony w przepisach rozporządzenia.

§ 17. Formularze dokumentów stosowane dotychczas jako druki stale mogą być wykorzystywane do wyczerpania zapasów, nie dłużej jednak niż do dnia 31 grudnia 2012 r.

§ 18. Rozporządzenie wchodzi w życie z dniem 1 stycznia 2012 r.

Prezes Rady Ministrów: D. Tusk

Aneks nr 4[89]

ROZPORZĄDZENIE RADY MINISTRÓW
z dnia 29 maja 2012 r.
w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych
(Dz.U. z 2012 r. poz. 683)

Na podstawie art. 47 ust. 1 pkt 1 i 3–6 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228) zarządza się, co następuje:

§ 1.1. Rozporządzenie określa:
1) podstawowe kryteria i sposób określania poziomu zagrożeń;
2) dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;
3) rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń;
4) podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;
5) zakres stosowania środków bezpieczeństwa fizycznego;
6) kryteria tworzenia stref ochronnych.

2. Przepisów rozporządzenia regulujących sprawy, o których mowa w ust. 1 pkt 2 i 5, nie stosuje się w jednostkach organizacyjnych organów wymienionych w art 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą", oraz w stosunku do informacji niejawnych wchodzących w skład zasobu archiwalnego archiwów państwowych. W jednostkach organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2 ustawy, nie stosuje się ponadto przepisów rozporządzenia regulujących sprawy, o których mowa w ust. 1 pkt 4 i 6.

§ 2. Ilekroć w rozporządzeniu jest mowa o:
1) dostępności informacji niejawnej – należy przez to rozumieć właściwość określającą, że informacja niejawna jest możliwa do wykorzystania na żądanie podmiotu uprawnionego w określonym czasie;
2) integralności informacji niejawnej – należy przez to rozumieć właściwość określającą, że informacja niejawna nie została zmodyfikowana w sposób nieuprawniony;
3) poufności informacji niejawnej – należy przez to rozumieć właściwość określającą, że informacja niejawna nie jest ujawniana podmiotom do tego nieuprawnionym;

[89] Interpunkcja w tekście zgodna z oryginałem. Ze względu na charakter i przeznaczenie niniejszej publikacji nie podano treści załączników do rozporządzenia – nr 1: Podstawowe kryteria i sposób określania poziomu zagrożeń, oraz nr 2: Metodyka doboru środków bezpieczeństwa fizycznego.

4) incydencie bezpieczeństwa – należy przez to rozumieć pojedyncze zdarzenie lub serię zdarzeń związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności.

§ 3.1. W ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności tych informacji.

2. W celu doboru adekwatnych środków bezpieczeństwa fizycznego określa się poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zwany dalej „poziomem zagrożeń".

3. Poziom zagrożeń określa się dla pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne.

4. Poziom zagrożeń określa się jako wysoki, średni albo niski.

5. Przy określaniu poziomu zagrożeń uwzględnia się:

1) zagrożenia naturalne, wynikające z działania sił przyrody lub awarii urządzeń;
2) zagrożenia związane zarówno z umyślnym, jak i nieumyślnym zachowaniem człowieka.

6. W celu określenia poziomu zagrożeń przeprowadza się analizę, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych.

7. Poziom zagrożeń określa się przed rozpoczęciem przetwarzania informacji niejawnych, a także po każdej zmianie czynników, o których mowa w ust. 6.

8. Podstawowe kryteria i sposób określania poziomu zagrożeń zawiera załącznik nr l do rozporządzenia.

§ 4.1. Cel, o którym mowa w § 3 ust 1, osiąga się przez:

1) zapewnienie właściwego przetwarzania informacji niejawnych;
2) umożliwienie zróżnicowania dostępu do informacji niejawnych dla pracowników zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji niejawnych;
3) wykrywanie, udaremnianie lub powstrzymywanie działań nieuprawnionych;
4) uniemożliwianie lub opóźnianie wtargnięcia osób nieuprawnionych w sposób niezauważony lub z użyciem siły do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne.

2. Środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje niejawne, z zastrzeżeniem § 8 ust. 5.

3. System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych. W zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy, o której mowa w § 3 ust. 6, stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

1) personel bezpieczeństwa – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji

niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na alarmy lub sygnały awaryjne;
2) bariery fizyczne – środki chroniące granice miejsca, w którym są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;
3) szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;
4) system kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;
5) system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;
6) system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;
7) system kontroli osób i przedmiotów – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

4. W celu zapewnienia poufności, integralności i dostępności informacji niejawnych można zastosować również środki bezpieczeństwa fizycznego inne niż wymienione w ust. 3, jeżeli taka potrzeba wynika z analizy poziomu zagrożeń.

5. Jeżeli istnieje zagrożenie podglądu, także przypadkowego, informacji niejawnych, zarówno w świetle dziennym, jak i w warunkach sztucznego oświetlenia, podejmuje się działania w celu wyeliminowania takiego zagrożenia.

6. Elektroniczny system pomocniczy wspomagający ochronę informacji niejawnych powinien posiadać wydane przez dostawcę, z uwzględnieniem przepisów o systemie oceny zgodności, poświadczenie zgodności z wymogami określonymi w rozporządzeniu.

7. Metodykę doboru środków bezpieczeństwa fizycznego określa załącznik nr 2 do rozporządzenia.

§ 5.1. Tworzy się następujące strefy ochronne:
1) strefę ochronną I – obejmującą pomieszczenie lub obszar, w których informacje niejawne o klauzuli „poufne" lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośred-

niego dostępu do tych informacji; pomieszczenie lub obszar spełniają następujące wymagania:
   a) wyraźnie wskazana w planie ochrony najwyższa klauzula tajności przetwarzanych informacji niejawnych,
   b) wyraźnie określone i zabezpieczone granice,
   c) wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych,
   d) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. c, przetwarzane informacje niejawne zabezpiecza się przed możliwością dostępu do nich tych innych osób oraz zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne,
   e) wstęp możliwy jest wyłącznie ze strefy ochronnej;
2) strefę ochronną II – obejmującą pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne" lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji; pomieszczenie lub obszar spełniają następujące wymagania:
   a) wyraźnie określone i zabezpieczone granice,
   b) wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych,
   c) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. b, zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne,
   d) wstęp możliwy jest wyłącznie ze strefy ochronnej;
3) strefę ochronną III – obejmującą pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów;
4) specjalną strefę ochronną – umiejscowioną w obrębie strefy ochronnej I lub strefy ochronnej II, chronioną przed podsłuchem, spełniającą dodatkowo następujące wymagania:
   a) strefę wyposaża się w system sygnalizacji włamania i napadu,
   b) strefa pozostaje zamknięta, gdy nikogo w niej nie ma,
   c) w przypadku posiedzenia niejawnego strefa jest chroniona przed wstępem osób nieupoważnionych do udziału w tym posiedzeniu,
   d) strefa podlega regularnym inspekcjom przeprowadzanym według zaleceń Agencji Bezpieczeństwa Wewnętrznego albo Służby Kontrwywiadu Wojskowego, nie rzadziej niż raz w roku oraz po każdym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście mogło mieć miejsce,
   e) w strefie nie mogą znajdować się linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny, których

umieszczenie nie zostało zaakceptowane w sposób określony w procedurach bezpieczeństwa, o których mowa w § 9 ust. 1 pkt 4.

2. Pomieszczenie lub obszar w każdej strefie ochronnej, w których praca nie odbywa się w systemie całodobowym, sprawdza się bezpośrednio po zakończeniu pracy w celu upewnienia się, że informacje niejawne zostały właściwie zabezpieczone.

3. W strefie ochronnej I lub w strefie ochronnej II można utworzyć pomieszczenie wzmocnione. Konstrukcja pomieszczenia powinna zapewniać ochronę równoważną ochronie zapewnianej przez odpowiednie szafy przeznaczone do przechowywania informacji niejawnych o tej samej klauzuli tajności. W pomieszczeniu wzmocnionym dopuszczalne jest przechowywanie informacji niejawnych poza odpowiednimi szafami.

4. Strefę ochronną I, strefę ochronną II lub specjalną strefę ochronną można utworzyć tymczasowo w strefie ochronnej III w celu odbycia posiedzenia niejawnego.

§ 6. Klucze i kody dostępu do szaf, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, mogą być udostępnione tylko tym osobom, którym posiadanie kluczy lub znajomość kodów są niezbędne do wykonywania obowiązków służbowych. Kody zmienia się co najmniej raz w roku, a także w przypadku:

1) każdej zmiany składu osób znających kod;
2) zaistnienia podejrzenia, że osoba nieuprawniona mogła poznać kod;
3) gdy zamek poddano konserwacji lub naprawie.

§ 7.1. Informacje niejawne o klauzuli „ściśle tajne" przetwarza się w strefie ochronnej I lub w strefie ochronnej II i przechowuje się w szafie metalowej spełniającej co najmniej wymagania klasy odporności na włamanie S2, określone w Polskiej Normie PN-EN 14450 lub nowszej, lub w pomieszczeniu wzmocnionym, z zastosowaniem jednego z poniższych środków uzupełniających:

1) stała ochrona lub kontrola w nieregularnych odstępach czasu przez pracownika personelu bezpieczeństwa posiadającego odpowiednie poświadczenie bezpieczeństwa, w szczególności z wykorzystaniem systemu dozoru wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni;
2) system sygnalizacji włamania i napadu obsługiwany przez personel bezpieczeństwa z wykorzystaniem systemu dozoru wizyjnego, o którym mowa w pkt 1.

2. Informacje niejawne o klauzuli „tajne" przetwarza się w strefie ochronnej I lub w strefie ochronnej II i przechowuje się w szafie metalowej spełniającej co najmniej wymagania klasy odporności na włamanie Sl, określone w Polskiej Normie PN-EN 14450 lub nowszej, lub w pomieszczeniu wzmocnionym.

3. Informacje niejawne o klauzuli „poufne":
1) przetwarza się w strefie ochronnej I, II lub III;
2) przechowuje się w strefie ochronnej I lub w strefie ochronnej II w szafie metalowej lub w pomieszczeniu wzmocnionym.

4. Informacje niejawne o klauzuli „zastrzeżone" przetwarza się w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu i przechowuje się w szafie metalowej, pomieszczeniu wzmocnionym lub zamkniętym na klucz meblu biurowym.

§ 8.1. Przetwarzanie informacji niejawnych o klauzuli „poufne" lub wyższej w systemach teleinformatycznych odbywa się w strefie ochronnej I lub w strefie ochronnej II, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

2. Przekazywanie informacji, o których mowa w ust. 1, odbywa się w strefie ochronnej, na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

3. Przetwarzanie informacji niejawnych o klauzuli „zastrzeżone" w systemach teleinformatycznych odbywa się w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

4. Serwery, systemy zarządzania siecią, kontrolery sieciowe i inne newralgiczne elementy systemów teleinformatycznych umieszcza się, z uwzględnieniem wyników procesu szacowania ryzyka, o którym mowa w art 49 ust l ustawy, w następujący sposób:
1) w strefie ochronnej w przypadku przetwarzania informacji niejawnych „zastrzeżone".
2) w strefie ochronnej I lub w strefie ochronnej II, w przypadku przetwarzania informacji niejawnych o lub wyższej.

5. Przetwarzanie informacji niejawnych w części mobilnej zasobów systemu teleinformatycznego odbywa się na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy, w sposób określony w dokumentacji bezpieczeństwa systemu teleinformatycznego.

§ 9.1. Kierownik jednostki organizacyjnej zatwierdza plan ochrony informacji niejawnych, który zawiera:
1) opis stref ochronnych, pomieszczeń lub obszarów, o których mowa w § 7 ust. 4, w tym określenie ich granic i wprowadzonego systemu kontroli dostępu;
2) procedury zarządzania uprawnieniami do wejścia, wyjścia i przebywania w strefach ochronnych;
   e) opis zastosowanych środków bezpieczeństwa fizycznego uwzględniający certyfikaty, o których mowa w art. 46 pkt 4 ustawy, oraz poświadczenia, o których mowa w § 4 ust. 6;
4) procedury bezpieczeństwa dla strefy ochronnej I, strefy ochronnej II oraz specjalnej strefy ochronnej, określające w szczególności:

a) klauzule tajności informacji niejawnych przetwarzanych w strefie,
b) sposób sprawowania nadzoru przez osoby uprawnione w przypadku przebywania w strefie osób nieposiadających stałego upoważnienia do wstępu oraz sposób zabezpieczania przetwarzanych informacji niejawnych przed możliwością nieuprawnionego dostępu tych osób,
c) w przypadku specjalnej strefy ochronnej, sposób akceptacji umieszczania linii komunikacyjnych, telefonów, innych urządzeń komunikacyjnych, sprzętu elektrycznego lub elektronicznego, znajdujących się w strefie;

5) procedury zarządzania kluczami i kodami dostępu do szaf, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne;
6) procedury reagowania osób odpowiedzialnych za ochronę informacji niejawnych oraz personelu bezpieczeństwa w przypadku zagrożenia utratą lub ujawnieniem informacji niejawnych;
7) plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych, w celu zapobieżenia utracie poufności, integralności lub dostępności informacji niejawnych.

2. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych plan, o którym mowa w ust. 1, może zawierać dodatkowe elementy.

§ 10.1. W terminie 3 lat od dnia wejścia w życie rozporządzenia określa się poziom zagrożeń, opracowuje dokumenty, o których mowa w § 9, i dostosowuje się kombinację środków bezpieczeństwa fizycznego oraz organizację stref ochronnych do wymagań określonych w rozporządzeniu.

2. Certyfikaty i tabliczki znamionowe przyznane wyposażeniu i urządzeniom służącym ochronie informacji niejawnych, wydane przed dniem wejścia w życie rozporządzenia, zachowują ważność.

§ 11. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów: D. Tusk

Część druga
Ochrona danych osobowych

1. Ochrona prawno-administracyjna

Prywatność jest jedną ze sfer naszego życia, którą cenimy sobie najbardziej. Prawo do prywatności, choć nie jest wymienione *expressis verbis* w art. 23 Kodeksu cywilnego, należy też do tych wartości niematerialnych, które wymagają poszanowania. Jego ochrona wynika zaś z przepisów prawa krajowego i międzynarodowego, takich jak:

- art. 8, Europejska konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r. […] (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)[1];
- art. 17, Międzynarodowy pakt praw obywatelskich i politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167)[2];
- art. 31, 47 i 51, Konstytucja RP z dnia 2 kwietnia 1997 r.[3].

---

[1] „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego swojego mieszkania i swojej korespondencji"; „Niedopuszczalna jest ingerencja władzy publicznej w korzystaniu z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobiegania przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób".

[2] „Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani tez na bezprawne zamachy na jego cześć i dobre imię".

[3] W art. 31 ust. 3 Konstytucji RP zapisano, że ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanowione tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego oraz nie naruszają istoty tych wolności i praw. Z kolei w art. 47 ust. 1 gwarantuje się każdemu prawo do „ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym", natomiast w art. 49 zapewnia się „wolność i ochronę tajemnicy komunikowania się", a w art. 51 zapisano, iż „1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych do-

Jakąkolwiek ingerencję w sprawy rodzinne, osobiste lub intymne zwykle postrzegamy jako coś negatywnego i niepożądanego, mimo to skłonni jesteśmy zaakceptować, że gromadzenie pewnych informacji o nas jest niezbędne dla prawidłowego funkcjonowania wielu instytucji publicznych, lecz oczekujemy, że do naszych danych osobowych[4], będących w posiadaniu tych instytucji, nie będą miały dostępu osoby niepowołane. Naruszenia prywatności przez dostęp do zbiorów danych osobowych były powodem stworzenia regulacji prawnych gwarantujących ochronę prywatności, a jednocześnie zapewniających bezpieczeństwo informacji o obywatelach.

2. Regulacje prawne dotyczące tworzenia i posługiwania się zbiorami danych osobowych

Na płaszczyźnie międzynarodowej

Pierwszą na świecie ustawę o ochronie danych osobowych uchwalił federalny parlament Hesji w 1970 r. W chwili obecnej takie regulacje prawne posiadają już wszystkie kraje europejskie, a także Stany Zjednoczone i Kanada.

Najstarszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych jest Konwencja nr 108 Rady Europy z 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28 stycznia 1981 r. (Dz.U. z 2003 r. Nr 3, poz. 25)[5].

Konwencja ta nałożyła na kraje członkowskie zobowiązanie stworzenia ustawodawstwa w zakresie ochrony danych osobowych, wskazując jednocześnie, w jakim kierunku ustawodawstwo to ma zmierzać.

Celem konwencji jest zapewnienie na obszarze państw członkowskich każdemu – niezależnie od obywatelstwa i zamieszkania – ochrony jego praw i wolności, a w szczególności prawa do poszanowania sfery osobistej w związku z automatycznym przetwarzaniem danych osobowych. Konwencja określiła minimalny zakres tych praw i skorelowanych z nimi obowiązków. Konwencja weszła w życie l października 1985 r.

---

kumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa". Nasza prywatność jest także wprost chroniona przez przepisy Prawa prasowego, które stanowią, iż „nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba, że wiąże się to bezpośrednio z działalnością publiczną danej osoby" (art. 14 ust. 6 pp).

4 W rozumieniu Ustawy o ochronie danych osobowych za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

5 Ratyfikowana przez Polskę 24 kwietnia 2002 r.

Początkowo Unia Europejska nie dostrzegała konieczności uregulowania kwestii ochrony danych osobowych w krajowych, szczegółowych aktach prawnych. Komisja Europejska postulowała jedynie, aby państwa członkowskie ratyfikowały konwencję do 1982 r.

Z czasem jednak rozbieżności w ustawodawstwie państw UE spowodowały konieczność ich ujednolicenia. Zasadniczym zadaniem, jaki taka regulacja miała spełnić, było zapewnienie minimalnego, a zarazem jednolitego dla państw członkowskich, poziomu ochrony danych osobowych gromadzonych w zbiorach oraz zapewnienie swobodnego przepływu danych osobowych pomiędzy krajami członkowskimi.

Zrealizowanie tego drugiego zadania jest koniecznym dalszym warunkiem zapewnienia swobodnego przepływu towarów, usług i osób pomiędzy krajami UE, co każdorazowo łączy się z koniecznością przekazania danych osobowych.

W 1990 r. rozpoczęto prace nad stosowną dyrektywą. Efektem tych prac było wydanie dokumentu Dyrektywa Parlamentu Europejskiego i Rady nr 95/46/EC z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz.UE L 281 z 23.11.1995 z późn. zm.). Termin na jej implementację do porządków prawnych państw członkowskich wyznaczono na 23 października 1998 r.

Dyrektywa przyjęła bardzo szerokie rozumienie pojęcia danych osobowych oraz przetwarzania danych. Danymi osobowymi określiła wszystkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przetwarzaniem zaś określiła wszystkie, wymieniając je, operacje dokonywane na danych osobowych. Wprowadziła katalog minimalnych praw służących osobom, których dane są zbierane. Ich naruszenie miałoby skutkować możliwością dochodzenia tych praw na drodze sądowej. Dopuszczalność przetwarzania danych została uzależniona od woli (zgody) osoby, której dotyczą dane osobowe. Przewidziano jednak zamknięty katalog sytuacji, gdy jest to możliwe bez takiej zgody. Dyrektywa wyodrębnia grupę danych osobowych tzw. sensytywnych. W przypadku ich przetwarzania wymagana jest zgoda wyrażona na piśmie. Odrębnie potraktowano też dane dotyczące skazań kryminalnych, które mogą być przetwarzane jedynie przez podmioty publiczne. Sprecyzowano, kiedy możliwe jest odstępstwo od zasady zakazu przetwarzania takich danych.

Jednocześnie, zgodnie z dyrektywą, dane mogą być wykorzystywane wyłącznie zgodnie z celem, dla którego zostały zgromadzone. Dyrektywa wprowadziła obowiązek informowania osoby o zasadach przetwarzania jej danych przed ich zgromadzeniem. Może ona sprzeciwić się przetwarzaniu swoich danych, jeśli tylko posiada w tym uzasadniony cel. Każda osoba, której dane już znalazły się w zbiorze, ma prawo dowiedzieć się o zasadach ich przetwarzania, począwszy od możliwości ustalenia informacji o administratorze, skończywszy na ustaleniu treści tych danych.

Dyrektywa wprowadziła też prawo kontroli danych osobowych przez osobę, której one dotyczą, w tym prawo wniesienia sprzeciwu przeciwko przetwarza-

niu danych. Osobie, która poniosła szkodę wynikającą z przetwarzania danych niezgodnie z dyrektywą, przysługuje odszkodowanie. Jedną z najważniejszych wprowadzonych regulacji jest kwestia przekazywania danych osobowych do krajów trzecich (jest to możliwe wtedy, gdy kraj docelowy zapewnia odpowiedni poziom ochrony).

Ponadto dyrektywa przewidziała powołanie krajowych organów nadzorczych. Ich zadaniem jest monitorowanie przestrzegania dyrektywy. Na podstawie art. 29 dyrektywy powołana została także Grupa Robocza ds. Ochrony Danych. W jej skład wchodzą przedstawiciele krajowych organów nadzorczych oraz przedstawiciel Komisji Europejskiej. Jej celem jest przyczynianie się do jednolitego stosowania dyrektywy w krajach członkowskich, opiniowanie istniejącego poziomu ochrony danych w różnych krajach oraz opiniowanie unijnych aktów normatywnych z zakresu ochrony prywatności na potrzeby Komisji Europejskiej

Dyrektywa przewidziała też powołanie komitetu doradczego, złożonego z przedstawicieli krajów członkowskich. Jego zadaniem jest projektowanie i opiniowanie nowych aktów normatywnych z zakresu uregulowanego dyrektywą.

Z kolei w późniejszych latach ukazały się jeszcze:

- Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w dziedzinie telekomunikacji (Dz.Urz.UE L 24 z 30.01.1998).
- Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (Dz.Urz.UE L 178 z 17.07.2000).
- Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. 2002/58/WE w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej) (Dz.Urz.UE L 201 z 31.07.2002).
- Dyrektywa Parlamentu Europejskiego i Rady WE z dnia 15 marca 2006 r. 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.Urz.UE L 105 z 13.04.2006).
- Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych dotyczący organów nadzoru i transgranicznych przepływów danych, sporządzony w Strasburgu dnia 8 listopada 2001 r. (Dz.U. z 2006 r. Nr 3, poz. 15).

W systemie prawa polskiego

W Polsce ochrona danych osobowych jest nową dziedziną prawa. Wprowadzenie jej jest efektem akceptacji wielu międzynarodowych umów i traktatów dotyczących praw człowieka do prywatności. Ochronę danych osobowych w skrócie można by określić jako ochronę możliwości decydowania przez daną osobę

fizyczną o tym, jakie informacje o niej mogą być pozyskiwane i udostępniane innym osobom.

Aktualnie o obowiązku ochrony danych osobowych stanowią:

- wspomniane art.: 31, 47 i 51 Konstytucji RP z dnia 2 kwietnia 1997 r.
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135).
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2013 r. poz. 1422).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r. Nr 229, poz. 1536).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. z 2014 r. poz. 1934).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. z 2015 r. poz. 719).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r. poz. 745).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 2004 r. Nr 94, poz. 923).
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011 r. Nr 225, poz. 1350).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2004 r. Nr 94, poz. 923 z późn. zm.).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2014 r. Nr 100, poz. 1024), określające:

  - sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
  - podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
  - wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r. Nr 229, poz. 1536).

3. Kogo dotyczy przedmiotowa ustawa?

Zakres obowiązywania ustawy o ochronie danych osobowych określony został w art. 2 i 3, a mianowicie ustawę stosuje się do przetwarzania danych osobowych:

a) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych;
b) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych[6];
c) organów państwowych, organów samorządu terytorialnego oraz dopaństwowych i komunalnych jednostek organizacyjnych;
d) podmiotów niepublicznych realizujących zadania publiczne;
e) osób fizycznych i osób prawnych oraz jednostek organizacyjnych niemających osobowości prawnej, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub czynią to dla realizacji celów statutowych[7] które mają siedzibę albo miejsce zamieszkania na terytorium RP, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium RP.

---

[6] 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 poddawanych anonimizacji, mają zastosowanie jedynie zasady ich zabezpieczenia.

[7] Danymi osobowymi są np. dane osobowe gromadzone przez pracodawcę w formie akt, a także informacje o kredytobiorcach. Zgodnie z ustawą każde przedsiębiorstwo zatrudniające choćby jednego pracownika lub przetwarzające inne dane osobowe musi dysponować dokumentacją przetwarzania danych osobowych (określoną w § 3 ust. 1 Rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych), polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Brak takiej dokumentacji może się wiązać z nałożeniem grzywny w wysokości do 50 tys. zł.

Ustawa nie ma natomiast zastosowania do:

a) osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych;
b) podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium RP wyłącznie do przekazywania danych;
c) prasowej działalności dziennikarskiej[8], literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

4. Rodzaje danych osobowych

1. Z art. 6 ust. 1 uodo (definicji danych osobowych) wynika, że dana informacja ma charakter osobowy, jeżeli wiemy, kogo ona dotyczy, lub nie wiemy, ale bez trudu możemy to określić, bezpośrednio lub pośrednio, przez powołanie się na jej numer identyfikacyjny albo jeden lub kilka czynników określających jej cechy (fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne[9].
2. Do rzędu danych osobowych zalicza się również informacje o dochodach i zadłużeniu konkretnej osoby[10], o tym czyim dana osoba jest klientem/pa-

---

8 W rozumieniu Prawa prasowego.

9 Prywatność może również zostać naruszona przez każdą wypowiedź o charakterze informacyjnym. Nie jest istotne przy tym, czy rozpowszechniana informacja jest prawdziwa, czy też fałszywa, ponieważ nawet spekulacja odnośnie do życia prywatnego innej osoby może naruszać omawiane dobro. Prywatność zostanie także pogwałcona przez opublikowanie wizerunku utrwalonego w prywatnej sytuacji. Zaznaczyć należy ponadto, iż ochrona prywatności nie ustaje nawet po ujawnieniu prywatnych danych. Odpowiedzialność za naruszenie prywatnej sfery życia będzie ponosić także osoba, której działanie polegało jedynie na powtarzaniu tych wiadomości.

10 A zatem rozpowszechnianie takich informacji należy traktować w kategoriach naruszenia danych osobowych. Powyższe znajduje swoje potwierdzenie w orzecznictwie Sądu Najwyższego, który uznał, że wysokość zarobków poszczególnych pracowników jest tajna, a ich udostępnienie jest naruszeniem dóbr osobistych (zob. Uchwała SN z 16 lipca 1993 r., I PZP 28/93, OSNC 1994/1/2). Czyli dokumenty zawierające informacje o wysokości wynagrodzenia mogą zostać udostępnione do wglądu jedynie pracownikowi, którego dotyczą. Pracownik, którego prawa zostały naruszone (np. rozpowszechniono informacje o wysokości jego zarobków), może domagać się od pracodawcy odszkodowania i stosownego zadośćuczynienia. Niezależnie od odpowiedzialności cywilnej pracodawca, w którego firmie doszło do bezprawnego rozpowszechniania danych osobowych, takich jak: informacje o wysokości wynagrodzenia pracowników, naraża się na odpowiedzialność za złamanie przepisów Ustawy o ochronie danych osobowych. Istnieją sytuacje, w których zainteresowanie życiem prywatnym danej osoby może być usprawiedliwione z powodu zajmowanego przez nią stanowiska. Dotyczy to osób powszechnie znanych, biorących udział w życiu publicznym. Zdaniem Naczelnego Sądu Administracyjnego we Wrocławiu (Wyrok z 6 maja 1997 r., II SA/Wr 929/96, ONSA 1998/2/54) wysokość wynagrodzenia członków zarządu gminy (wójta, burmi-

cjentem, z kim wiąże ją stosunek prawny o charakterze ciągłym, adres poczty elektronicznej[11], a także – niekiedy – jej wizerunek[12].

3. Dane te mogą przybierać różną formę utrwalenia i występować w postaci notatki, zdjęć, filmów, zarejestrowanych głosów (fonoskopii) lub za pomocą badań struktury kwasu DNA[13].
4. Zgodnie z poglądami wyrażonymi w piśmiennictwie charakter danych osobowych posiadają informacje z różnych dziedzin życia, o ile tylko istnieje możliwość powiązania ich z określoną osobą.
5. W ustawie o ochronie danych osobowych nie pojawiają się takie pojęcia, jak „dane zwykłe" i „dane wrażliwe" (sensytywne), ale taki podział dyktuje ich bezpośrednie użycie, a także ma miejsce w wielu interpretacjach GIODO.

Mówiąc najprościej, dane wrażliwe to informacje, które mogą zostać wykorzystane przeciwko interesom danej osoby przez ich ujawnienie, udostępnienie lub zmanipulowanie, a których przetwarzanie jest poddane ochronie i szczególnemu trybowi. Wszelkie inne dane osobowe nazywamy danymi zwykłymi.

---

strza i ich zastępców) nie należy wyłącznie do sfery prywatności osób piastujących te stanowiska, gdyż wiąże się z ich funkcją publiczną. Na zasadzie art. 4 ust. 2 w związku z art. 14 ust. 6 pp organ gminy nie może odmówić redaktorom prasowym udzielenia informacji o wysokości wynagrodzenia za pracę osób piastujących te stanowiska. Zatem pełnienie określonych funkcji publicznych w organach władzy państwowej lub samorządowej skutkuje jawnością wynagrodzeń tych osób. Jawności takiej nie można jednak stosować wobec pracowników, którzy nie pełnią funkcji publicznych. Ochronie danych osobowych nie podlegają również informacje o wynagrodzeniu kadry kierowniczej spółek państwowych (art. 15 tzw. ustawy kominowej, tj. Ustawy z dnia 3 marca 2000 r. o wynagrodzeniu osób kierujących niektórymi podmiotami prawnymi [Dz.U. z 2000 r. Nr 26, poz. 306 z późn. zm.]). Tak samo co do zasady jawne są wynagrodzenia członków zarządów spółek giełdowych. Zarówno przepisy, jak i zasady dobrej praktyki wymagają, aby publikować je w raportach rocznych. Obecnie podaje się zarobki każdego menedżera z osobna, choć wcześniejszą praktyką było ujawnianie ich łącznie dla całego zarządu.

[11] Danymi osobowymi nie są więc pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy i numer domu, w którym mieszka wiele osób, czy wysokość wynagrodzenia. Informacja taka będzie stanowić dane osobowe, gdy zostanie zestawiona z innymi danymi, np. imieniem i nazwiskiem czy numerem PESEL pracownika. Podobnie adres poczty elektronicznej, bez dodatkowych informacji, umożliwiających ustalenie tożsamości osoby, zasadniczo nie stanowi danych osobowych. Występujący samodzielnie adres poczty elektronicznej można jednak – w wyjątkowych przypadkach – uznać za dane osobowe, ale tylko wtedy, gdy elementy jego treści pozwalają, bez nadmiernego wysiłku (kosztów, czasu lub działań) na ustalenie na ich podstawie tożsamości danej osoby. Dzieje się tak w sytuacji, gdy elementami treści adresu są np. imię i nazwisko jego właściciela.

[12] Wizerunek osoby staje się chronioną prawem jedną z danych osobowych dopiero wtedy, gdy daje się go powiązać z określoną osobą i został rozpowszechniony bez zgody osoby sfotografowanej.

[13] K. Napierała, *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach teleinformatycznych*, Warszawa 1997, s. 21.

Przykładowo danymi zwykłymi są: imię i nazwisko, adres zamieszkania, wykształcenie, numer ewidencyjny (identyfikacyjny) (PESEL)[14].

W rozumieniu art. 27 uodo danymi wrażliwymi są informacje ujawniające:

a) pochodzenie rasowe lub etniczne;
b) poglądy polityczne;
c) przekonania religijne lub filozoficzne;
d) stan zdrowia;
e) przynależność partyjną, związkową lub wyznaniową;
f) kod genetyczny;
g) nałogi;
h) życie i orientację seksualną;
i) skazania i orzeczenia dotyczące mandatów i kar, a także inne wydane w postępowaniu sądowym lub administracyjnym.

Jeśli zaś chodzi o kwestię rozpowszechniania wizerunku osób bez ich zgody, to sprawę reguluje Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90, poz. 631), która w art. 81 ustanawia zasadę, iż rozpowszechnianie wizerunku jakiejś osoby wymaga jej zgody.

Jako rozpowszechnianie należy z kolei rozumieć jakiekolwiek udostępnianie publiczne fotografii, np. umieszczanie jej na wystawie, stronie internetowej, w gazecie itp. Zakłada się m.in., że zgoda taka została wyrażona, gdy osoba, której wizerunek będzie rozpowszechniany, otrzymała za to zapłatę. Od powyższej zasady przewidziane są jednak dwa wyjątki, nie jest bowiem wymagana zgoda na rozpowszechnianie wizerunku osoby powszechnie znanej lub jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych. Ponadto zgoda taka nie jest wymagana od osoby stanowiącej jedynie szczegół całości, takiej jak: zgromadzenie, krajobraz, publiczna impreza itp., bądź gdy jej widok będzie szczegółem jakiejś całości, np. widok przechodniów na ulicy.

Powyższe uregulowania dotyczą jedynie rozpowszechniania wizerunku. Pamiętać jednak należy, że wizerunek, w świetle przepisów art. 22 Kodeksu cywilnego, stanowi dobro osobiste każdego człowieka i jako takie podlega ochronie. Jednakże ochrona ta nie jest tak daleko idąca jak przy opisanym powyżej rozpowszechnianiu czyjegoś wizerunku, do którego wymagana jest wyraźna zgoda portretowanej osoby.

Można więc przyjąć, iż w przypadku, gdy fotografia nie będzie rozpowszechniana, wyraźna zgoda portretowanej osoby nie jest wymagana. Wystarczająca wydaje się tu zgoda domniemana – którą możemy przyjąć, gdy portretowana

---

[14] Numer PESEL (Powszechny Elektroniczny System Ewidencji Ludności) jest to 11-cyfrowy stały symbol numeryczny jednoznacznie identyfikujący określoną osobę fizyczną. Zbudowany jest z następujących elementów: zakodowanej daty urodzenia (dwóch ostatnich cyfry roku, miesiąca i d), liczby porządkowej z zakodowanym oznaczeniem płci i cyfry kontrolnej. Numer PESEL nadaje minister właściwy do spraw wewnętrznych w formie czynności materialno-technicznej. Nadanie numeru PESEL następuje za pośrednictwem urzędu gminy właściwego ze względu na miejsce zamieszkania.

osoba, mając tego świadomość, nie sprzeciwia się temu wyraźnie, ale gdy osoba taka sprzeciwi się fotografowaniu, będzie to wiążące dla fotografa, bowiem fotografowanie, filmowanie takiej osoby stanowić będzie naruszenie jej dobra osobistego, co uprawniać będzie ją np. do żądania zaprzestania dalszych naruszeń, a także odszkodowania czy zadośćuczynienia.

Także zapis obrazu i dźwięku z monitoringu tworzy zestaw danych osobowych, który po spełnieniu określonych warunków[15] może być zbiorem danych w rozumieniu art. 7 ust. 1 uodo[16].

6. Danymi osobowymi nie są informacje o osobach zmarłych, gdyż zakresem przedmiotowym Ustawy o ochronie danych osobowych objęte są wyłącznie dane dotyczące osób fizycznych.

5. Przetwarzanie danych osobowych

Art. 7 uodo jest zbiorem pojęć ustawowych, gdzie przez przetwarzanie danych rozumie się 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.

1. Zgodnie ze wspomnianą wcześniej Konwencją Rady Europy dane osobowe powinny być:
   a) pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem[17];
   b) gromadzone dla określonych i usprawiedliwionych celów i nie mogą być wykorzystywane w sposób niezgodny z tymi celami;

---

[15] Przykłady sytuacji, w jakich nagranie z monitoringu może być uznane za zbiór danych osobowych, to: a) zestaw danych został poddany opracowaniu (skatalogowaniu), w wyniku którego utworzono indeksy umożliwiające dotarcie do zapisu danych konkretnej osoby, b) system informatyczny stosowany w związku z monitoringiem wyposażony został w mechanizmy umożliwiające automatyczne wyszukanie w zarejestrowanych nagraniach danych dotyczących konkretnej osoby (np. mechanizm rozpoznawania kształtu twarzy, sylwetki, głosu); c) dotarcie do danych konkretnej osoby jest możliwe na podstawie innego zbioru danych osobowych, w którym rejestrowane są w sposób tradycyjny zdarzenia z udziałem konkretnej osoby, zarejestrowane równocześnie w zapisie z monitoringu (np. w kasynach gry, gdzie monitoring stosowany przy wejściu do budynku połączony jest z tradycyjną księgą wejść/wyjść).

[16] Zbiór danych osobowych to termin prawniczy, który oznacza każdy posiadający strukturę zestaw danych o charakterze osobowym, niezależnie od tego, czy jest rozproszony lub podzielony funkcjonalnie. Cechą, która wyróżnia zbiór danych od innego zestawu danych, jest jego struktura, czyli takie jego uporządkowanie, które daje możliwość wyszukania konkretnych danych według określonych kryteriów. 1) Dostępność do danych osobowych w zbiorze danych musi być możliwa na podstawie co najmniej dwóch kryteriów. 2) Ze zbiorem danych osobowych mamy do czynienia, gdy łatwo jest się dostać do wielu informacji o konkretnych osobach.

[17] Jednym z kryteriów objęcia danych osobowych prawną ochroną jest to, że figurują one w jakimś zestawie (zbiorze) danych.

c) odpowiednie, rzeczowe i niewykraczające poza potrzeby, dla których są gromadzone;
d) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego je zgromadzono.

2. Wdrożenie tych zasad opiera się na trzech fundamentalnych elementach:
   a) stworzeniu struktury zarządzania procesami przetwarzania danych osobowych – wyznaczeniu ról zarządczych i kontrolnych;
   b) stworzeniu dokumentacji opisującej zasady przetwarzania i ochrony danych osobowych;
   c) przeszkoleniu wszystkich osób upoważnionych do przetwarzania danych z zasad ich ochrony oraz dodatkowo osób zarządzających i kontrolujących – z zadań w ramach zarządzania procesami ich przetwarzania.
3. Polskie zasady przetwarzania danych osobowych zostały uregulowane w rozdziale 3 uodo, głównie w art. 26, który nakłada na administratora danych obowiązek dołożenia szczególnej staranności w celu ochrony interesów (majątkowych i niemajątkowych) osób, których dane dotyczą, a w szczególności przestrzegania następujących zasad: legalności, celowości, merytorycznej poprawności, adekwatności oraz ograniczenia czasowego.
   a) Zasada legalności zostanie zachowana, jeżeli administrator danych, dokonując przetwarzania danych zwykłych, zachowa przynajmniej jedną z wymienionych w art. 23 uodo przesłanek dopuszczalności przetwarzania danych. Te przesłanki to:
      - zgoda osoby, której dane dotyczą[18], chyba że chodzi o usunięcie danych;
      - niezbędność realizacji uprawnień lub spełnienia obowiązku wynikającego z przepisu prawa;
      - konieczność realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy przetwarzanie jest niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
      - niezbędność przetwarzania danych do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
      - niezbędność przetwarzania danych dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której one dotyczą; w przypadku danych szczególnie chronionych (danych wrażliwych) z zasady ich przetwarzanie jest zabronione, a dopuszczalne jest tylko po zaistnieniu jednej z poniżej wymienionych przesłanek:

[18] Istotne jest, żeby zgoda osoby, której dane dotyczą, wyrażona w postaci oświadczenia woli na przetwarzanie danych, była zgodą wyraźną, zdecydowaną, nie zaś domniemaną lub dorozumianą i dotyczyła wyłącznie przetwarzania danych (art. 7 pkt 5 uodo). Zgoda może obejmować również przetwarzanie danych w przyszłości, pod warunkiem jednak, że nie zmienia się cel przetwarzania. Jeżeli natomiast przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody jest utrudnione bądź niemożliwe, ustawa dopuszcza przetwarzanie danych bez zgody tej osoby jednak tylko do czasu, gdy uzyskanie zgody będzie możliwe.

- osoba, której dane dotyczą wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
- przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
- przetwarzanie takich danych jest niezbędne dla 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;
- jest to niezbędne do wykonywania 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;
- przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
- przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
- 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;
- przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
- 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;
- przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym[19].

b) Zasada związania z celem w praktyce oznacza, że zbierający dane nie może pominąć ani zataić celu zbierania przed osobą, która te dane udostępnia. Osoba udostępniająca dane powinna być poinformowana o celu zbierania

[19] Stosowanie zasady legalności oznacza nie tylko zachowywanie przepisów Ustawy o ochronie danych osobowych, ale także wszystkich przepisów prawa. Należy podkreślić, że zasada legalności nie obejmuje postanowień umownych.

danych przed ich udostępnieniem. Cel ten nie może być określony w sposób ogólnikowy i niejasny, mogący wprowadzić w błąd. Niedopuszczalne jest uzależnianie zawarcia umowy od wyrażenia zgody na przetwarzanie danych w innych celach, np. marketingowych czy innych podmiotów[20].

c) Zasada merytorycznej poprawności – zapewnienie merytorycznej poprawności danych osobowych w praktyce oznacza, że dane te mają być zgodne z prawdą, kompletne i aktualne. Realizacja tego obowiązku wymaga, żeby administrator danych każdorazowo oceniał wiarygodność źródła danych i ustalił zasady postępowania w sytuacji stwierdzenia nieprawidłowości.

O uaktualnieniu lub sprostowaniu danych administrator ma obowiązek niezwłocznie poinformować tego administratora, który udostępnił mu zbiór danych. Naruszeniem tej zasady jest zbieranie danych niewiadomego pochodzenia, które nie gwarantują ich poprawności, oraz taka konstrukcja programów komputerowych, która powodowałaby konieczność przetwarzania danych nieprawdziwych, nieaktualnych czy niekompletnych[18].

d) Zasada adekwatności. Administrator danych powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, jakie są niezbędne ze względu na cel zbierania danych. Ocena tego, jakie dane będą zbierane, musi nastąpić przed rozpoczęciem ich zbierania. W ocenie tej powinien być uwzględniony stosunek prawny, w związku z którym administrator przetwarza dane osobowe[21].

e) Zasada ograniczenia czasowego oznacza w praktyce, że po osiągnięciu celu – np. wykonaniu umowy, upływie wynikającego z przepisów prawa okresu przechowywania danych – dane powinny zostać usunięte, poddane anonimizacji lub też przekazane podmiotowi uprawnionemu ustawowo do ich przejęcia (np. archiwum państwowemu). W związku z tym administrator jest zobowiązany do stałego przeglądania podległych mu danych pod kątem realizacji tej zasady[22].

---

[20] Wyjątkiem od zasady celowości – jak już wcześniej wspomniano – jest przetwarzanie danych w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, pod warunkiem że nie narusza to praw i wolności osoby, której dane dotyczą, oraz następuje z zachowaniem przepisów art. 23 i 25 uodo.

[21] W odniesieniu do umów należy zaś uwzględnić ich charakter i znaczenie. W niektórych bowiem sytuacjach przepisy prawa wprost wskazują zakres danych adekwatnych w celu przetwarzania i w takich przypadkach zbieranie danych wykraczających poza wskazany zakres jest niedopuszczalne. Naruszeniem tej zasady jest także zbieranie danych „na wszelki wypadek". Warto zwrócić uwagę, że posłużenie się określoną techniką zbierania danych, np. wykonywaniem kserokopii dokumentów, nie przesądza o naruszeniu tej zasady.

[22] 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

f) Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych (art. 32 uodo), a zwłaszcza prawo do:
   - 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;
   - uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
   - uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
   - uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej;
   - uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
   - 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;
   - wniesienia pisemnego umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;
   - wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

g) Do obsługi systemu informatycznego oraz wchodzących w jego skład urządzeń służących do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych (art. 37 uodo).

h) Osoby upoważnione do przetwarzania danych osobowych obowiązane są do zachowania w tajemnicy danych i sposobów ich zabezpieczenia (art. 39 uodo).

4. Dokumentację przetwarzania danych stanowią:
   a) polityka bezpieczeństwa;

---

usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy. Kiedy administrator odmawia wypełnienia tego obowiązku, osoba, której dane dotyczą składa wniosek do GIODO, a ten wydaje decyzję administracyjną nakazującą przywrócenie stanu zgodnego z prawem.

b) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

5. Polityka bezpieczeństwa jest zbiorem wewnętrznych regulacji związanych z przetwarzaniem danych osobowych obowiązujących w danej jednostce organizacyjnej. Prowadzona jest w formie opisowej i zawiera:
   a) opis celów, zasad i standardów ochrony danych w instytucji przetwarzającej dane osobowe;
   b) wykaz budynków, pomieszczeń i miejsc, które razem tworzą obszar, w którym przetwarzane są dane osobowe[23];
   c) wykaz zbiorów danych osobowych[24] wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
   d) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   e) sposób przepływu danych pomiędzy poszczególnymi systemami;
   f) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
6. Instrukcja zarządzania systemem informatycznym zawiera w szczególności:
   a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
   b) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
   c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
   d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   e) sposób, miejsce i okres przechowywania:
      - elektronicznych nośników informacji zawierających dane osobowe;
      - kopii zapasowych zbiorów danych.
   f) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego;
   g) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
7. Przetwarzanie danych wrażliwych dopuszczalne jest wyłącznie w przypadkach wymienionych w ustawie, mianowicie gdy:
   a) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie;

---

[23] Wykaz powinien obejmować zarówno pomieszczenia, w których wykonuje się czynności związane z przetwarzaniem danych, jak i pomieszczenia, w których przechowuje się nośniki, na których znajdują się dane osobowe.

[24] Zbiór danych to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów (art. 7 ust. 1 uodo).

b) inna ustawa zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
c) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów;
d) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
e) jest to niezbędne do prowadzenia badań naukowych, pod warunkiem anonimizacji danych.

8. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia, wprowadzono następujące poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: podstawowy, podwyższony i wysoki[25]:
   a) poziom co najmniej podstawowy stosuje się, gdy:
      - w systemie informatycznym nie są przetwarzane tzw. dane wrażliwe;
      - żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
   b) poziom co najmniej podwyższony stosuje się, gdy:
      - w systemie informatycznym przetwarzane są dane wrażliwe;
      - żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
   c) poziom wysoki stosuje się zaś, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.

6. Podmioty procesu przetwarzania danych osobowych

1. Osobami uczestniczącymi w procesie przetwarzania danych osobowych są:
   a) administrator danych (osoba zarządzająca procesem zbierania i przetwarzania danych);
   b) odbiorca danych;
   c) podmiot, któremu powierzono przetwarzanie danych;
   d) administrujący zbiorem danych;
   e) administrator bezpieczeństwa informacji (ABI);
   f) administrator bezpieczeństwa systemów.
2. Administratorem danych jest osoba fizyczna lub prawna, organ państwowy bądź organ samorządu terytorialnego, który sprawuje władztwo nad przetwarzaniem danych – decyduje o celach i środkach przetwarzania danych osobowych (art. 7 pkt 4 uodo)[26].

---

[25] Szerzej zob. Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych.

[26] W przypadku danych pracowników administratorem danych w stosunku do zbioru zawierającego ich dane osobowe będzie pracodawca. Osoba fizyczna jest administratorem danych tylko w sytuacji, gdy przetwarza dane osobowe na własny rachunek i to tylko w sytuacji przetwarzania związanego z działalnością zarobkową lub zawodową, np. w sytuacji realizowania umowy o dzieło. Osoba fizyczna nie będzie administratorem w sytu-

Do administratora danych osobowych należy:

a) obowiązek umożliwienia kontroli w miejscu przechowywania danych osobowych inspektorom biura GIODO (art. 15 ust. 1 uodo);
b) obowiązek informacyjny wypełniany w stosunku do tych, których dotyczą przetwarzane dane osobowe (art. 24, 25, 32, 33 i 54 uodo)[27];
c) szczególna staranność przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza (art. 26 uodo);
d) obowiązek uzupełniania, uaktualnienia, prostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane przez administratora (art. 35 uodo);
e) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (art. 36 uodo);
f) obowiązek kontroli, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane (art. 38 uodo);
g) obowiązek prowadzenia ewidencji i szkolenie osób upoważnionych do przetwarzania danych osobowych (art. 39 uodo);

---

acji przetwarzania danych wyłącznie w celach osobistych lub domowych, ponieważ przepisy wyłączają stosowanie ustawy w takiej sytuacji (art. 3a pkt 1 uodo). Administratorem danych osobowych nie jest również podmiot, któremu zostało powierzone przetwarzanie danych osobowych (np. nie jest nim agent ubezpieczeniowy, który gromadzi dane dla towarzystwa ubezpieczeniowego).

[27] Niezależnie od wspomnianych zasad przetwarzania danych osobowych ustawa zobowiązuje administratora danych do poinformowania osoby, której dane dotyczą o: 1) adresie swojej siedziby i pełnej nazwie, 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. W przypadku natomiast zbierania danych osobowych od osoby, której one nie dotyczą, oprócz podania ww. danych, do poinformowania o źródle pochodzenia danych, uprawnieniach zezwalających na wniesienie pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, wniesienia sprzeciwu wobec przetwarzania jej danych, gdy administrator danych zamierza przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych. W niektórych przypadkach ustawa zwalnia administratora danych z obowiązku informowania osoby, w szczególności zaś gdy: a) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą (np. przez policję, służby specjalne czy organy administracji finansowej, b) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub do badania opinii publicznej, c) ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a informowanie osób wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu przetwarzania (art. 25 ust. 2 pkt 3 uodo).

   h) zgłoszenie zbioru do rejestracji GIODO (art. 40 uodo)[28];
   i) obowiązek zgłaszania (w terminie 30 dni) GIODO każdej zmiany w zbiorze informacji (art. 41 uodo).
3. Odbiorcą danych jest osoba, której udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą;
   b) osoby upoważnionej do przetwarzania danych;
   c) przedstawiciela administratora danych, gdy przetwarzanie danych odbywa się poza miejscem jego zamieszkania lub w państwie trzecim;
   d) osoby przetwarzającej dane w drodze umowy z administratorem danych[29].
4. Administrator bezpieczeństwa informacji to osoba wyznaczona przez administratora danych do sprawowania nadzoru i kontroli nad przestrzeganiem zasad ochrony danych osobowych przed ich udostępnieniem osobom nieuprawnionym, nieuprawnioną ich zmianą, utratą, uszkodzeniem lub zniszczeniem[30].
   Administrator bezpieczeństwa informacji jest *de facto* prawą ręką administra-

[28] Zgłoszenie zbioru danych do rejestracji powinno zawierać: 1) wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych, 2) oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w rym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku podmiotu, o którym mowa w art. 31a, oznaczenie tego podmiotu i adres jego siedziby lub miejsce zamieszkania, 3) cel przetwarzania danych, 4) opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych, 5) sposób zbierania oraz udostępniania danych, 6) informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane, 7) opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36–39 uodo, 8) informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a uodo, 9) informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego (art. 41 uodo).

[29] Odmowa udostępnienia danych osobowych przez administratora danych podmiotom i osobom innym niż uprawnionym na mocy ustawy następuje w przypadku, gdy spowodować by to mogło ujawnienie wiadomości zawierających informacje niejawne, zagrożenie dla obronności lub bezpieczeństwa, życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

[30] Wyznaczenie ABI jest fakultatywne. W przypadku niepowołania ABI, czynności jemu przypisane wykonuje administrator danych osobowych. Ustawa o ochronie danych osobowych nie stanowi o tym wyraźnie, jednak przyjmuje się, że administrator bezpieczeństwa informacji powinien być osobą fizyczną. Ponadto nie jest wymagane, aby ABI był pracownikiem administratora danych. Dlatego osoba pełniąca tę funkcję może zostać dobrana spoza grona pracowników administratora danych. Nie ma bowiem przeszkód, aby ABI wykonywał swoje czynności jako przedsiębiorca w ramach samozatrudnienia lub też jako pracownik zatrudniony u pracodawcy innego niż podmiot występujący w roli administratora danych.

tora danych w zakresie ochrony wszystkich informacji przetwarzanych w organizacji. Katalog jego zadań i kompetencji jest duży i obejmuje (art. 26 ust. 1 uodo):

a) Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe, oraz kontrolą przebywających w nich osób. Pomieszczenia, o których mowa, powinny być zabezpieczone przed dostępem do nich osób nieposiadających uprawnień do przetwarzania danych osobowych. Osoby nieposiadające takich uprawnień mogą przebywać w nich jedynie w obecności osób uprawnionych. Na czas nieobecności zatrudnionych tam osób pomieszczenia te powinny być odpowiednio zabezpieczone. W celu zabezpieczenia pomieszczeń należy zastosować odpowiednie zamki do drzwi oraz sprawować właściwy nadzór nad kluczami do tych pomieszczeń.
b) Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. Komputery oraz urządzenia, o których mowa wyżej, powinny być zasilane przez zastosowanie specjalnych urządzeń podtrzymujących zasilanie. Urządzenia te powinny być wyposażone w oprogramowanie umożliwiające bezpieczne wyłączenie systemu komputerowego. Oznacza to takie wyłączenie, w którym przed zanikiem zasilania zostaną prawidłowo zakończone rozpoczęte transakcje na bazie danych oraz wszelkie inne działania w ramach pracujących aplikacji i oprogramowania systemowego.
c) Dopilnowanie, aby komputery przenośne, w których przetwarzane są dane osobowe, były zabezpieczone hasłem dostępu przed nieautoryzowanym uruchomieniem oraz, aby mikrokomputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych. Osoby posiadające mikrokomputery przenośne z zapisanymi w nich danymi osobowymi należy przeszkolić w kierunku zachowania szczególnej uwagi podczas ich transportu oraz uczulić na to, aby mikrokomputery te przechowywane były we właściwie zabezpieczonym pomieszczeniu.
d) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe. Dyski i inne informatyczne nośniki danych, zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a jeśli nie jest to możliwe, należy uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisu danych osobowych lub naprawiać w obecności osoby upoważnionej przez administratora danych.
e) Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które powinny być zawarte w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
f) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.

g) Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.
h) Nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych.
i) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.
j) Nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny. W zakresie nadzoru, o którym mowa, administrator bezpieczeństwa informacji powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub już niepotrzebnych wydruków komputerowych z danymi osobowymi.
k) Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych. Nadzorowanie, o którym mowa, powinno obejmować:
   - ustalenie identyfikatorów użytkowników i ich haseł (identyfikatory użytkowników należy wpisać do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych);
   - dopilnowanie, aby hasła użytkowników były zmieniane co najmniej raz na miesiąc;
   - dopilnowanie, aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła;
   - dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy (również po upływie terminu ich ważności);
   - dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych, zostały natychmiast wyrejestrowane, a ich hasła unieważnione;
   - dopilnowanie, aby – jeżeli istnieją odpowiednie możliwości techniczne – ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika. Zalecanym rozwiązaniem powyższego problemu jest zastosowanie takich wygaszaczy ekranowych, które po upływie określonego czasu bezczynności użytkownika wygaszają monitor i jednocześnie uruchamiają blokadę uniemożliwiającą kontynuowanie pracy na komputerze bez podania właściwego hasła. Wygaszacz taki, oprócz ochrony danych, które przez dłuższy czas byłyby wyświetlane na ekranie monitora, chroniłby system przed przechwyceniem sesji dostępu do danych przez nieuprawnioną osobę;

- dopilnowanie, aby w pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych były ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

l) Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa, powinny mieć na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie.

m) Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło), i przygotowanie oraz przedstawienie administratorowi danych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych. Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości. Obowiązek śledzenia skuteczności zabezpieczeń, o którym mowa wyżej, oraz obowiązek ich udoskonalania, nałożony na administratora bezpieczeństwa, wynika bezpośrednio z obowiązku podejmowania odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

5. Administrator bezpieczeństwa systemu informatycznego (ABSI) odpowiada zaś za wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę systemu informatycznego służącego do przetwarzania danych osobowych.

7. Organy ochrony danych osobowych

1. Centralnym organem ds. ochrony danych osobowych jest GIODO[31] powoływany na 4-letnią kadencję przez Sejm za zgodą Senatu.
2. Na stanowisko GIODO może być powołany ten, kto łącznie spełnia następujące warunki:
   a) jest obywatelem polskim i stale zamieszkuje na terytorium RP;
   b) wyróżnia się wysokim autorytetem moralnym;
   c) posiada wyższe wykształcenie prawnicze oraz odpowiednie doświadczenie zawodowe;
   d) nie był karany za przestępstwo.
3. Ta sama osoba nie może być GIODO więcej niż przez dwie kadencje.
4. GIODO nie może zajmować innego stanowiska, z wyjątkiem stanowiska profesora szkoły wyższej, ani wykonywać innych zajęć zawodowych.
5. GIODO nie może należeć do partii politycznych, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu. Nie może też być, bez uprzedniej zgody Sejmu, pociągnięty do odpowiedzialności karnej ani pozbawiony wolności, zatrzymany lub aresztowany,

[31] Adres Biura GIODO: ul. Stawki 2, 00-193 Warszawa.

z wyjątkiem ujęcia go na gorącym uczynku przestępstwa. O jego zatrzymaniu powiadamia się marszałka sejmu, który może nakazać jego natychmiastowe zwolnienie.

6. GIODO w zakresie wykonywania swoich zadań podlega tylko ustawie. Kadencja GIODO wygasa z chwilą jego śmierci, odwołania lub utraty obywatelstwa polskiego.
7. Sejm za zgodą Senatu odwołuje GIODO, jeżeli:
   a) zrzekł się stanowiska;
   b) stał się niezdolny do pełnienia obowiązków na skutek choroby;
   c) sprzeniewierzył się złożonemu ślubowaniu;
   d) został skazany prawomocnym wyrokiem sądu za popełnienie przestępstwa;
8. Do zadań GIODO w szczególności należy (art. 12 uodo):
   a) kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
   b) wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonywania przepisów o ochronie danych osobowych;
   c) prowadzenie rejestru zbiorów danych oraz udzielania informacji o zarejestrowanych zbiorach;
   d) opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych;
   e) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
   f) uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.
9. Uprawnienia GIODO wykonują w szczególności upoważnieni pracownicy biura – inspektorzy GIODO. Mają oni prawo:
   a) wstępu (od 6.00 do 22.00), za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczeń, w których znajduje się zbiór danych, i prowadzenia tam niezbędnych badań;
   b) żądania złożenia pisemnych lub ustnych wyjaśnień, a także wzywania i przesłuchiwania osoby w celu ustalenia stanu faktycznego;
   c) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii;
   d) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych;
   e) zlecać sporządzanie ekspertyz i opinii.
10. Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli oraz spełnić jego żądania, o których była mowa.
11. W toku kontroli zbiorów inspektor przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej.

12. Z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu administratorowi danych. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi. 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 GIODO.
13. Jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do GIODO o zastosowanie przewidzianych prawem środków.
14. 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.
15. W przypadku naruszenia przepisów o ochronie danych osobowych GIODO z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:
    a) usunięcie uchybień;
    b) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;
    c) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;
    d) wstrzymanie przekazywania danych osobowych do państwa trzeciego;
    e) zabezpieczenie danych lub przekazanie ich innym podmiotom;
    f) usunięcie danych osobowych.
16. Decyzje GIODO nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa.
17. W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa, GIODO kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.
18. GIODO składa Sejmowi raz w roku sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych.

8. Rejestracja i aktualizacja zbiorów danych

Proces zgłoszenia zbiorów danych do rejestracji GIODO oraz ich aktualizacja wynikają bezpośrednio z przepisów Ustawy o ochronie danych osobowych. Zbiory należy zgłaszać do rejestracji przed rozpoczęciem przetwarzania na specjalnym formularzu określonym w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do

rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Należy również aktualizować każdą informację podaną w zgłoszeniu rejestracyjnym w ciągu 30 dni od zajścia zmiany[32].

Z obowiązku rejestracji zbiorów danych zwolnieni są administratorzy danych:

a) objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego;
b) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności;
c) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym;
d) przetwarzanych przez GIIF;
e) dotyczących osób należących do Kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego Kościoła lub związku wyznaniowego;
f) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się;
g) dotyczących osób korzystających z usług medycznych w zespołach opieki zdrowotnej[33], obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta;
h) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd prezydenta RP, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego;
i) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności;
j) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
k) powszechnie dostępnych;
l) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego;
m) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

---

[32] Formularz wniosku jest dostępny na stronie internetowej GIODO – www.giodo.gov.pl. Zgłoszenie zbioru danych do rejestracji może być dokonane za pośrednictwem poczty, osobiście lub przy wykorzystaniu elektronicznej platformy komunikacji e-giodo, dostępnej ze strony internetowej GIODO, pod warunkiem posiadania przez podmiot zgłaszający podpisu elektronicznego.

[33] Niedopuszczalne jest natomiast umieszczanie na drzwiach gabinetu lekarskiego listy nazwisk pacjentów zapisanych na dany dzień do lekarza; w odniesieniu do danych wrażliwych, tj. szczególnie chronionych – art. 27 ust. 1 uodo oraz art. 40 ust. 4 Ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz.U. z 2015 r. poz. 464).

9. Przepisy karne

Przewidziany ustawą zakres penalizacji jest bardzo szeroki i tak[34]:

Art. 49.

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. 51.

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.

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.

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

Art. 54.

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.

Ponadto na mocy Ustawy z dnia 29 października 2010 r o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz.U. z 2010 r. Nr 229, poz. 1497) GIODO przyznano uprawnienia organu egzekucyjnego w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym (art. 1 pkt. 2 dotyczący zmiany art. 12 uodo). Oznacza to, że GIODO na podmioty, które nie wykonują jego decyzji administracyjnych, może nakładać grzywnę w celu ich przymuszenia. Wysokość takiej grzywny w stosunku do osoby fizycznej może wynieść maksymalnie 10 tys. zł, zaś w stosunku do osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej 50 tys. zł, jednak w przypadku wielokrotnego nakładania grzywien w jednym postępo-

[34] Art. 49–54 uodo. Interpunkcja w tekście zgodna z oryginałem.

waniu egzekucyjnym ich łączna kwota nie będzie mogła przekraczać: 50 tys. zł w odniesieniu do osób fizycznych oraz 200 tys. zł w odniesieniu do osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej.

Grzywny te GIODO może nakładać w trybie przewidzianym Ustawą z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz.U. z 2014 r. poz. 1619 z późn. zm.).

Pytania kontrolne

1. Wymień wobec kogo stosuje się Ustawę o ochronie danych osobowych?
2. Co w rozumieniu ustawy uważa się za dane osobowe?
3. Co obejmuje proces przetwarzania danych osobowych i jakich danych nie można przetwarzać?
4. Wymień prawa osób, których dane dotyczą?
5. Jakie czyny, określone w Ustawie o ochronie danych osobowych, podlegają karze grzywny, ograniczenia albo pozbawienia wolności?

Bibliografia

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011.

Dyrektywa Parlamentu Europejskiego i Rady nr 95/46/EC z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz.UE L 281 z 23.11.1995 z późn. zm.).

Europejska konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r. […] (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.).

Międzynarodowy Konwencja nr 108 Rady Europy z 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28 stycznia 1981 r. (Dz.U. z 2003 r. Nr 3, poz. 25).

Międzynarodowy pakt praw obywatelskich i politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).

Napierała K., *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach teleinformatycznych*, Warszawa 1997.

Ochrona danych osobowych wczoraj, dziś, jutro, Biuro GIODO, Warszawa 2006.

Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VIII Kongresu, red. M. Gajos, Katowice 2012.

Polok M., *Bezpieczeństwo danych osobowych*, Warszawa 2008.

Przegląd. Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informatycznych. W kierunku kultury bezpieczeństwa, OECD, 2003, dostępne na: www.oecd.org.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz

warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r. Nr 229, poz. 1536).

Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011 r. Nr 226, poz. 1350).

Szałowski R., *Ochrona danych osobowych – komentarz do ustawy*, Zielona Góra 2000.

Uchwała Sądu Najwyższego z 16 lipca 1993 r., I PZP 28/93, OSNC 1994/1/2.

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 1964 r. Nr 16, poz. 93 z późn. zm.).

Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz.U. z 2014 r. poz. 1619 z późn. zm.).

Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24 z późn. zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90, poz. 631).

Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz.U. z 2015 r. poz. 464).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r. Nr 133, poz. 883 z późn. zm., t.j. Dz.U. z 2015 r. poz. 2135, 2281, Dz.U. z 2016 r. poz. 195).

Ustawa z dnia 3 marca 2000 r. o wynagrodzeniu osób kierujących niektórymi podmiotami prawnymi (Dz.U. z 2000 r. Nr 26, poz. 306 z późn. zm.).

Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz.U. z 2010 r. Nr 229, poz. 1497).

Wyrok Naczelnego Sądu Administracyjnego we Wrocławiu z 6 maja 1997 r., II SA/Wr 929/96, ONSA 1998/2/54.

Część trzecia
Systemy informacyjne Schengen (SIS i VIS) a ochrona informacji niejawnych i danych osobowych

14 czerwca 1985 r. pięć państw członkowskich UE (Belgia, Holandia, Luksemburg, Niemcy oraz Francja) podpisały umowę o stopniowym znoszeniu kontroli na granicach wewnętrznych znaną jako Układ z Schengen mający urzeczywistnić zasadę swobodnego przepływu osób. W kolejnych latach do Układu z Schengen przystępowały kolejne państwa członkowskie UE: w 1990 r. – Włochy, w 1991 r. – Hiszpania i Portugalia, w 1992 r. – Grecja, w 1995 r. – Austria, w 1996 r. – Dania, Finlandia i Szwecja. Uczestnikami strefy Schengen zostały także państwa niebędące członkami UE – Norwegia i Islandia. Największe rozszerzenie strefy nastąpiło w 2007 r. w związku z przyjęciem do UE Polski, Czech, Estonii, Litwy, Łotwy, Malty, Słowacji, Słowenii i Węgier. Obecnie, po włączeniu Szwajcarii w 2008 r., do uczestnictwa w strefie Schengen przygotowują się Cypr, Bułgaria i Rumunia oraz Chorwacja. Zniesienie kontroli granicznych między państwami UE, które nastąpiło w nocy z 20 na 21 grudnia 2007 r., stanowiło urzeczywistnienie idei obszaru wspólnotowego bez barier fizycznych dla swobody przepływu osób i towarów oraz jednolitej polityki wizowej i współpracy sądowo-policyjnej państw. Jednocześnie w celu zapewnienia bezpieczeństwa i uniemożliwienia przemieszczania się w tym obszarze niepożądanych osób spoza strefy Schengen 19 czerwca 1990 r. przyjęto Konwencję wykonawczą do Układu z Schengen, ustanawiającą kontrolę nad takimi osobami w postaci Systemu Informacyjnego Schengen (SIS) i Wizowego Systemu Informacyjnego (VIS).

Zgodnie z art. 93 KWS celem systemów SIS i VIS jest utrzymanie porządku oraz bezpieczeństwa publicznego, łącznie z bezpieczeństwem narodowym, na terytoriach państw członkowskich oraz stosowanie postanowień Konwencji Wykonawczej Schengen dotyczących przepływu osób na tych terytoriach. Dane wprowadzone do systemów przez jedno państwo członkowskie dostępne są dla służb i organów pozostałych państw w niezbędnym dla nich zakresie. Systemy te zapewniają, za pomocą zautomatyzowanej procedury wyszukiwania, wymianę informacji pomiędzy służbami odpowiedzialnymi za ochronę granic, wydawanie wiz i bezpieczeństwo publiczne. Podczas przekraczania granic ze-

wnętrznych lub podczas standardowej kontroli policyjnej przy użyciu SIS następuje sprawdzenie, czy dany przedmiot (np. samochód) albo osoba figurują we wspólnej bazie danych.

W SIS przetwarzane są (art. 95–99 KWS):

- dane dotyczące osób poszukiwanych celem aresztowania ekstradycyjnego – w celu podjęcia działań zmierzających do wydania lub przekazania tej osoby;
- dane dotyczące cudzoziemców, którym odmawia się prawa wjazdu lub w celu wydalenia ich ze strefy Schengen;
- dane dotyczące osób zaginionych bądź osób, które dla ich własnej ochrony lub w celu zapobiegnięcia zagrożeniom należy tymczasowo oddać pod opiekę policji w celu poinformowania o danych ich dotyczących państwo wprowadzające wpis lub przetransportowania ich do bezpiecznego miejsca i zapobieżenia ich dalszej podróży;
- dane dotyczące świadków, osób wezwanych do stawienia się przed organami sądowymi w związku z postępowaniem karnym w celu poniesienia odpowiedzialności za swoje czyny, lub osób, które powinny odbywać wyrok w sprawie karnej lub wezwanych do stawienia się w celu odbycia kary pozbawienia wolności – w celu poinformowania państwo wprowadzające wpis o ich miejscu zamieszkania bądź pobytu;
- dane dotyczące osób lub pojazdów do celów niejawnego nadzoru lub szczególnych kontroli;
- dane dotyczące przedmiotów niezbędne do celów ich zajęcia lub wykorzystania w charakterze dowodu w postępowaniu karnym[1].

W odniesieniu do wymienionych osób i przedmiotów dopuszczalne jest przetwarzanie danych osobowych (art. 94 KWS), takich jak:

- imię i nazwisko, ewentualnie pseudonimy;
- inicjały drugich imion;
- stałe cechy wyglądu zewnętrznego;
- miejsce i datę urodzenia;
- płeć;
- narodowość;
- informacja, czy dana osoba jest uzbrojona, agresywna bądź jest uciekinierem;
- powód wpisania do SIS;
- informacja o działaniach, które należy przedsięwziąć wobec danej osoby[2].

---

[1] Do przedmiotów tych, zgodnie z ustępem 3 tego artykułu, zalicza się: pojazdy silnikowe o pojemności silnika przekraczającej 50 cm^3, które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone, przyczepy i naczepy o masie własnej przekraczającej 750 kg, które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone, broń palną, która została skradziona, wykorzystana w niewłaściwy sposób lub utracona, urzędowe blankiety, które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone, wydane dokumenty tożsamości (paszporty, dowody tożsamości, prawa jazdy), które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone, oraz podejrzane banknoty.

[2] Art. 94 ust. 1 KWS wskazuje jednocześnie, że przetwarzanie danych wrażliwych jest bezwzględnie zabronione.

Zgodnie z art. 109 KWS prawo dostępu do danych wprowadzonych do systemu wykonywane jest zgodnie z prawem krajowym umawiającej się strony, wobec której osoba fizyczna powołuje się na to prawo. Wskazać przy tym należy, że zgodnie z tym przepisem prawo krajowe strony może określać, czy krajowy organ nadzorczy określony na podstawie art. 114 ust. 1 KWS ma prawo decydować o tym, czy informacje mają zostać przekazane osobie, której dotyczą, oraz zgodnie z jakimi procedurami. Powyższy przepis reguluje jednocześnie sytuację, w której osoba fizyczna zamierza zrealizować prawo dostępu do danych w państwie stronie Konwencji wykonawczej do Układu z Schengen, która nie wprowadziła dotyczącej tej osoby wpisu. W takim przypadku strona niewprowadzająca wpisu musi przed przekazaniem danych umożliwić stronie wprowadzającej wpis wyrażenie swojego stanowiska.

Prawo dostępu do danych nie jest jednak prawem absolutnym i zgodnie z art. 109 ust. 2 KWS osoba fizyczna żądająca dostępu do danych przetwarzanych w SIS spotka się z odmową udostępnienia danych, jeżeli jest ona konieczna do wykonania zgodnego z prawem zadania w związku z wpisem bądź ze względu na ochronę praw i swobód stron trzecich. Ponadto zgodnie z art. 109 ust. 2 KWS *in fine* zabronione jest udostępnianie danych przetwarzanych ze względu na nadzór niejawny prowadzony na podstawie art. 99 KWS.

W wyniku realizacji prawa dostępu może okazać się, że przetwarzane dane są nieprawidłowe lub zostały przekazane niezgodnie z prawem. W takiej sytuacji osoba, której dane dotyczą, może skorzystać z przysługującego jej na podstawie art. 110 KWS prawa do żądania skorygowania tych danych bądź ich usunięcia.

Z powyższym przepisem związane są postanowienia art. 111 ust. 1 KWS stanowiącego, że każda osoba ma prawo wystąpić, na terytorium każdej z umawiających się stron, do sądów lub organów właściwych na mocy prawa krajowego z żądaniem poprawienia danych, ich usunięcia, uzyskania informacji lub uzyskania odszkodowania w związku z dotyczącym jej wpisem. Zgodnie z treścią ust. 2 tego przepisu umawiające się strony podejmują wspólnie działania w celu wykonania ostatecznego rozstrzygnięcia sądu bądź organu wskazanego w ust. 1. Za szkody spowodowane wykorzystaniem danych SIS odpowiedzialne jest zgodnie z prawem krajowym państwo będące stroną Konwencji wykonawczej do Układu z Schengen. Powyższy przepis art. 116 KWS stosuje się również do szkód wyrządzonych przez stronę, która wprowadziła wpis, jeżeli dane były niedokładne lub przechowywała dane niezgodnie z prawem.

Niezależnie od wskazanych powyżej praw każdej osobie przysługuje prawo zwrócenia się do krajowego organu nadzorczego wskazanego w art. 114 ust. 1 KWS, zgodnie z prawem krajowym strony, do której wniosek jest kierowany, o skontrolowanie dotyczących jej danych oraz sposobu ich wykorzystania. W przypadku wprowadzenia danych przez inną umawiającą się stronę kontrola, o którą zwraca się dana osoba, prowadzona jest w ścisłej koordynacji z organem nadzorczym strony, która wprowadziła określony wpis.

Zgodnie z treścią art. 101 KWS dostęp do danych wprowadzonych do SIS oraz prawo ich bezpośredniego przeglądania zastrzeżone są wyłącznie dla:

- organów odpowiedzialnych za kontrole graniczne oraz inne kontrole policyjne i celne prowadzone w ramach danego kraju, jak również koordynację takich kontroli;
- krajowych organów sądowniczych, w tym odpowiedzialnych za wszczęcie dochodzenia w ramach sądowego postępowania karnego i dochodzenia sądowego przed wniesieniem aktu oskarżenia oraz w zakresie dotyczącym wykonywania innych zadań, określonych przez ustawodawstwo krajowe;
- organów odpowiedzialnych za wydawanie wiz, centralnych organów odpowiedzialnych za rozpatrywanie wniosków wizowych oraz organów odpowiedzialnych za wydawanie dokumentów pobytowych, jak również za stosowanie prawodawstwa dotyczącego cudzoziemców w kontekście postanowień Konwencji wykonawczej do Układu z Schengen o przepływie osób;
- organów odpowiedzialnych za wydawanie dowodów rejestracyjnych pojazdów w celu ustalenia, czy określone pojazdy nie zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone.

Art. 112 KWS stanowi również, że dane osobowe przetwarzane w celu wykrywania osób powinny być przechowywane jedynie przez okres konieczny do osiągnięcia celów, dla których zostały wprowadzone. Strona, która wprowadziła wpis, musi najdalej w ciągu 3 lat od dnia wprowadzenia danych ocenić ich dalszą przydatność.

W przypadku nadzoru niejawnego osób prowadzonego na podstawie art. 99 KWS okres ten został zawężony do roku od dnia wprowadzenia danych. Wskazać przy tym należy, że zarówno okres 3-letni, jak i roczny nie wyznaczają czasu dozwolonego przetwarzania danych, ale jedynie wprowadzają konieczność okresowej oceny niezbędności danych w stosunku do celu ich przetwarzania[3].

VIS to system służący wymianie danych wizowych dotyczących wiz krótkoterminowych między państwami członkowskimi Schengen. System ten umożli-

[3] Rzeczywisty czas przetwarzania danych w SIS może być zatem krótszy bądź dłuższy, od terminu 3-letniego czy rocznego, i uzależniony jest od tego, czy udało się zrealizować cel, w jakim dane są przetwarzane w systemie. Przykładowo wskazać należy, że dane osobowe cudzoziemca, związane z odmową prawa wjazdu na terytorium Schengen obowiązującą np. przez 10 lat na podstawie prawomocnego wyroku, zostaną usunięte z systemu dopiero po 10 latach, przechodząc trzykrotnie okresowe badanie przydatności danych w stosunku do realizowanego celu. Powyższe terminy okresowego badania dopuszczalności przetwarzania danych należy uznać za okresy maksymalne, gdyż w myśl art. 112 ust. 2 KWS umawiające się strony mogą w prawie krajowym wprowadzić okresy krótsze. Na miesiąc przed zamierzonym usunięciem danych z systemu jednostka centralna systemu automatycznie informuje o tym stronę wprowadzającą wpis. W ciągu tego okresu strona ta może podjąć decyzję o zachowaniu wpisu. Wpisy, w stosunku do których strona wprowadzająca dany wpis nie uzna dalszej konieczności przetwarzania danych, są automatycznie usuwane.

wi upoważnionym władzom krajowym wprowadzanie i uaktualnianie danych wizowych oraz elektroniczną konsultację tych danych. Główne cele VIS to:

- uproszczenie procedury rozpatrywania wniosków wizowych;
- ułatwienie walki z nadużyciami;
- ułatwienie odpraw na przejściach granicznych na granicach zewnętrznych państw członkowskich i na terytoriach państw członkowskich;
- pomoc w identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium państw członkowskich lub też przestały spełniać te warunki;
- skuteczniejsze zapobieganie zagrożeniom bezpieczeństwa wewnętrznego każdego z państw członkowskich.

W systemie VIS rejestrowane są:

- dane osobowe oraz inne dane identyfikacyjne;
- fotografia osoby ubiegającej się o wizę;
- odciski palców;
- odsyłacze do innych wniosków, jeżeli wniosek wizowy zainteresowanej osoby został uprzednio zarejestrowany.

VIS został operacyjnie uruchomiony 11 października 2011 r. Jednakże rozpoczęcie funkcjonowania VIS nie zakończyło zadań związanych z jego pełnym wdrożeniem i przygotowaniem instytucji krajowych do współpracy z systemem, gdyż jest to proces wieloetapowy, rozciągnięty w czasie, mający na celu jego sukcesywne uruchamianie w kolejnych regionach świata oraz granicach zewnętrznych, a także zapewnienie dostępu dla służb odpowiedzialnych za zapobieganie, ściganie, zwalczanie przestępczości i terroryzmu. VIS jest oparty na scentralizowanej architekturze obejmującej Centralny Wizowy System Informacyjny, a także interfejs w każdym państwie oraz infrastrukturę komunikacyjną między Centralnym Wizowym Systemem Informacyjnym a interfejsami krajowymi. Za budowę wskazanych komponentów odpowiada Komisja Europejska, natomiast państwa są zobowiązane do dostosowania infrastruktury krajowej do współpracy z VIS. Zarządzanie VIS będzie realizowane na poziomie centralnym UE przez utworzoną w tym celu instytucję unijną, tę samą, co w przypadku SIS.

Udział Polski w SIS i VIS sankcjonuje i określa Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz.U. z 2007 r. Nr 165, poz. 1170), zgodnie z którą polskim administratorem danych przetwarzanych w systemach SIS i VIS, a jednocześnie odpowiedzialnym za sprawne działanie i bezpieczeństwo systemów, jest komendant główny Policji, i do niego należy zgłaszać wnioski o udostępnienie lub modyfikację danych.

Wykorzystywanie danych systemu SIS może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez obowiązku ujawniania faktycznego celu zbierania danych.

Aby zapewnić odpowiednią ochronę prawną osób, których dane są przechowywane w systemie SIS, GIODO sprawuje kontrolę nad tym, czy wykorzystywanie danych nie narusza praw osób, których dane te dotyczą. Kontrola ta jest sprawowana zgodnie z przepisami Ustawy o ochronie danych osobowych. Za szkody wyrządzone przez niezgodne z prawem wykorzystywanie danych SIS odpowiada Skarb Państwa, a organem reprezentującym Skarb Państwa w sprawach odszkodowawczych jest Prokuratoria Generalna Skarbu Państwa.

W myśl art. 118 KWS Polska zobowiązała się, w odniesieniu do swojego krajowego modułu SIS, przyjąć niezbędne środki w celu:

- odmowy nieupoważnionym osobom dostępu do sprzętu służącego przetwarzaniu danych osobowych (kontrola dostępu do sprzętu);
- zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji lub usuwaniu nośników danych (kontrola nośników danych);
- zapobiegania nieupoważnionemu wprowadzaniu danych oraz nieupoważnionym inspekcjom, modyfikacjom lub usuwaniu przechowywanych danych osobowych (kontrola gromadzenia danych);
- zapobiegania wykorzystywania zautomatyzowanych systemów przetwarzania danych przez nieupoważnione osoby z wykorzystaniem sprzętu do przekazywania danych (kontrola użytkownika);
- zapewnienia, aby osoby upoważnione do wykorzystywania zautomatyzowanych systemów przetwarzania danych miały jedynie dostęp do danych objętych ich upoważnieniem (kontrola dostępu do danych);
- zapewnienia możliwości weryfikacji i stwierdzania, do których organów dane osobowe mogą być przekazywane z wykorzystaniem sprzętu do przekazywania danych (kontrola transmisji danych);
- zapewnienia możliwości weryfikacji i stwierdzenia, które dane osobowe zostały wprowadzone do zautomatyzowanych systemów przetwarzania danych oraz kiedy i przez kogo dane zostały wprowadzone (kontrola dostarczania danych);
- zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji lub usuwaniu i danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola dostarczania danych).

Ze strony polskiej dostęp do systemów SIS i VIS mają:

- minister spraw wewnętrznych,
- komendant główny Policji,
- szef UdSC,
- SG,
- SC,
- Policja (w tym biuro SIRENE oraz personel Centralnego Organu Technicznego KSI),
- ABW,
- ŻW,
- CBA,
- organy kontroli skarbowej,
- sądy, prokuratorzy,

- wojewodowie,
- konsulowie,
- minister właściwy do spraw zagranicznych,
- starostowie (organy samorządowe właściwe w sprawach rejestracji pojazdów),
- BOR,
- AW,
- SWW,
- SKW,
- GIODO (w celu sprawowania kontroli nad tym, czy wykorzystywanie danych osobowych nie narusza praw osób, których dane te dotyczą [art. 9 uodo]).

Z powyższych rozważań wynika, że systemy SIS i VIS są ważnym elementem bezpieczeństwa państw strefy Schengen. Konwencja wykonawcza Układu z Schengen z 1985 r., będąca niejako jego konstytucją, składa się zarówno z wytycznych dotyczących tworzenia i funkcjonowania strefy, jak i przepisów zabezpieczenia, gwarantujących jej prawidłowe funkcjonowanie. Szczegółową regulacją i ograniczeniami objęto rodzaje informacji, które mogą być przetwarzane w ramach zbudowanego dlań systemu informacyjnego. I tak przyjęto, że:

1. Dane przetwarzane w systemie, wprowadzone zgodnie z art. 95–100 KWS, mogą być wykorzystywane jedynie do celów, dla których zostały wprowadzone, a które to cele zostały zdefiniowane we wskazanych przepisach.
2. Dane na temat osób poszukiwanych do aresztowania ekstradycyjnego są wprowadzane na wniosek władzy sądowej wzywającej strony Układu. Natomiast wpis do celów odmowy wjazdu – na podstawie wpisu krajowego wprowadzonego przez właściwe organy administracyjne.
3. Dostęp do danych wprowadzonych do SIS oraz prawo do ich bezpośredniego przeglądania mają wyłącznie organy odpowiedzialne za kontrole graniczne oraz inne kontrole policyjne i celne prowadzone w ramach danego kraju. Takie prawo mogą mieć również krajowe organy sądowe odpowiedzialne za wszczynanie postępowania karnego z oskarżenia publicznego.
4. Wykorzystywanie danych systemu SIS może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez obowiązku ujawniania faktycznego celu zbierania danych.
5. Dane, o których mowa, nie mogą być replikowane do zbiorów krajowych, z wyjątkiem tworzenia tzw. kopii technicznych – czyli zwielokrotnienia części zbioru danych, jeżeli jest to niezbędne w celu przeprowadzenia bezpośredniego przeglądu przez uprawnione organy.
6. Zabrania się przetwarzania tzw. danych wrażliwych.
7. Nie jest także dopuszczalne wykorzystanie danych zgromadzonych w SIS do celów administracyjnych, poza przypadkami wprost wskazanymi w Konwencji wykonawczej do Układu z Schengen.
8. Uzyskanie danych SIS w określonym państwie następuje w ramach modułu krajowego (N-SIS) przez dostęp do kopii zbioru danych zawartych w module

centralnym. Oznacza to, że żadne z państw nie ma bezpośredniego wglądu do danych zawartych w bazie systemu centralnego (C-SIS w Strasburgu) lub kopii krajowej innego państwa członkowskiego[4].

9. W kontekście okresu przechowywania danych w systemie nie wprowadzono co prawda sztywnego terminu, po którego upływie dane osobowe będą usuwane z systemu, przewidziano jednak mechanizm przeglądu takich danych po upływie 3 lat lub –w przypadku osób poddanych niejawnemu nadzorowi lub szczególnym kontrolom – jednego roku. W stosunku natomiast do przedmiotów okres przechowywania wynosi 10 lat, z tym że w przypadku pojazdów poddanych niejawnemu nadzorowi lub szczególnych kontroli – 5 lat.
10. Państwa członkowskie zobowiązane są do wyznaczenia krajowych organów nadzorczych, które sprawować będą niezależny nadzór nad danymi krajowego modułu SIS oraz kontrolę, czy przetwarzanie i wykorzystywanie danych nie narusza praw osób, których te dane dotyczą. Nadzór nad jednostką centralną SIS sprawowany z kolei jest przez wspólny organ nadzorczy, składający się z przedstawicieli wszystkich krajowych organów nadzorczych.
11. Ochrona danych osobowych odbywa się na podstawie prawa krajowego danego państwa członkowskiego. Dotyczy to także środków ochrony danych osobowych, a także cywilnoprawnych mechanizmów odszkodowawczych. Ogólnie ujmując, zarówno uprawnienia wynikające z reżimu ochrony danych osobowych, jak i roszczenia cywilnoprawne dochodzone mogą być na terytorium każdego z państw członkowskich, niezależnie od tego, czy adresatem takich żądań są organy tego czy innego państwa.
12. Zgodnie z regulacją, każde z państw zobowiązane jest do wykonania decyzji lub orzeczenia wydanego przez państwo, przed których żądania były dochodzone. Z kolei, to ostatnie, jest zobowiązane do wypłaty kwot zasądzonych tytułem odszkodowania, które to kwoty zostaną zwrócone przez państwo odpowiedzialne za wyrządzenie szkody, jeżeli nie było to państwo, w którym toczyło się postępowanie.

Pytania kontrolne

1. Co to jest Strefa Schengen i jakie sprawy reguluje Konwencja wykonawcza do Układu z Schengen?
2. Jakie są zasady działania Systemu Informacyjnego Schengen (SIS)?
3. Wymień zobowiązania Polski wobec danych SIS w strefie Schengen?

---

[4] Zawartość informacyjna zbiorów danych zgromadzonych w modułach krajowych jest synchronizowana ze zbiorem modułu centralnego za pomocą krajowego punktu kontaktowego – biura SIRENE (Supplementary Information Request at the National Entries) oraz systemu konsultacji wizowych, tzw. VISION. Przez nie też następuje komunikacja z innymi państwami.

Bibliografia

Konwencja wykonawcza do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 grudnia 2007 r. w sprawie trybu przekazywania Policji osób lub przedmiotów odnalezionych na skutek wglądu do danych SIS, a także związanych z tym obowiązków Policji (Dz.U. z 2007 r. Nr 235, poz. 1731).

Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (t.j. Dz.U. z 2015 r. poz. 2135, 2281, Dz.U. z 2016 r. poz. 195.)

Ustawa z 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen i Systemie Informacji Wizowej (Dz.U. z 2007 r. Nr 165, poz. 1170).

Widmański L., *System Informacyjny Schengen – podstawowy instrument funkcjonowania strefy Schengen*, 12.01.2009, dostępne na: www.edukacjaprawnicza.pl.

Aneks 1[5]

KONWENCJA WYKONAWCZA DO UKŁADU Z SCHENGEN
z dnia 14 czerwca 1985 roku
między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach
(fragment tekstu ujednoliconego – stan na 18.10.2013 r.)

TYTUŁ IV
SYSTEM INFORMACYJNY SCHENGEN

ROZDZIAŁ 1
UTWORZENIE SYSTEMU INFORMACYJNEGO SCHENGEN

Artykuł 92

1. Umawiające się Strony tworzą i prowadzą wspólny system informacyjny, zwany dalej „Systemem Informacyjnym Schengen", składający się z krajowych modułów w każdej z Umawiających się Stron oraz jednostki centralnej. System Informacyjny Schengen umożliwia organom wyznaczonym przez Umawiające się Strony, przy pomocy zautomatyzowanej procedury wyszukiwania, dostęp do wpisów dotyczących osób i majątku w celach kontroli granicznej oraz innych kontroli policyjnych i celnych prowadzonych w ramach danego kraju zgodnie z prawem krajowym oraz, w przypadku szczególnej kategorii wpisów określonych w artykule 96, w celach wydawania wiz, dokumentów pobytowych i wykonywania przepisów prawnych o cudzoziemcach w kontekście stosowania postanowień niniejszej Konwencji odnoszących się do przepływu osób.
2. Każda z Umawiających się Stron tworzy i prowadzi na własny rachunek i ryzyko swój własny krajowy moduł Systemu Informacyjnego Schengen, którego pliki danych powinny być merytorycznie takie same jak pliki danych krajowych modułów każdej z pozostałych Umawiających się Stron, przy pomocy jednostki centralnej. W celu zapewnienia szybkiego i efektywnego przekazywania danych określonych w ustępie 3 każda z Umawiających się Stron przy tworzeniu swojego krajowego modułu przestrzega protokołów i procedur, jakie Umawiające się Strony wspólnie ustanowiły dla jednostki centralnej. Pliki danych każdego krajowego modułu powinny być dostępne do celów prowadzenia automatycznego wyszukiwania na terytorium każdej z Umawiających się Stron. Dokonywanie przeglądu plików danych krajowych modułów Umawiających się Stron nie jest możliwe.
3. Umawiające się Strony tworzą i prowadzą, na zasadzie wspólnego ponoszenia kosztów oraz wspólnej odpowiedzialności, jednostkę centralną Systemu

[5] Interpunkcja i ortografia w tekście zgodna z oryginałem.

Informacyjnego Schengen. Republika Francuska odpowiada za jednostkę, która znajduje się w Strasburgu. Jednostka centralna zawiera pliki danych, które zapewniają, poprzez transmisję on-line, aby pliki danych krajowych modułów zawierały identyczne informacje. Pliki danych jednostki centralnej zawierają wpisy dotyczące osób i majątku w zakresie, w jakim dotyczy to wszystkich Umawiających się Stron. Pliki danych jednostki centralnej nie zawierają danych innych niż dane określone w niniejszym ustępie oraz w artykule 113 ustęp 2.

4. Państwa Członkowskie, zgodnie z ich prawem krajowym, wymieniają poprzez organy wyznaczone w tym celu (SIRENE) wszystkie informacje uzupełniające niezbędne przy wprowadzaniu wpisów i w celu umożliwienia podjęcia odpowiednich działań w przypadkach, gdy w wyniku przeglądania danych Systemu Informacyjnego Schengen odnaleziono osoby lub przedmioty, na temat których wprowadzono informacje do tego systemu. Informacje takie są wykorzystywane wyłącznie do celu, w jakim zostały przekazane.

ROZDZIAŁ 2
DZIAŁANIE I KORZYSTANIE Z SYSTEMU INFORMACYJNEGO SCHENGEN

Artykuł 93

Celem Systemu Informacyjnego Schengen jest, zgodnie z niniejszą Konwencją, utrzymanie porządku publicznego oraz bezpieczeństwa publicznego, włączając bezpieczeństwo narodowe, na terytoriach Umawiających się Stron oraz stosowanie postanowień niniejszej Konwencji odnoszących się do przepływu osób na tych terytoriach, z wykorzystaniem informacji przekazywanych za pośrednictwem niniejszego systemu.

Artykuł 94[6]

1. System Informacyjny Schengen zawiera jedynie te kategorie danych, które są dostarczane przez każdą z Umawiających się Stron, wymagane do celów ustanowionych w artykułach 95–100. Umawiająca się Strona wprowadzająca wpis określi, czy sprawa ta jest wystarczająco ważna dla wprowadzenia powyższego wpisu do Systemu Informacyjnego Schengen.

---

[6] Przed zapoznaniem się z treścią artykułu należy wspomnieć, iż:

- Z dniem 9 kwietnia 2013 r. art. 94 utracił moc w kwestiach wchodzących w zakres Traktatu ustanawiającego Wspólnotę Europejską, zgodnie z art. 52 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady nr 1987/2006 z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz.UE L 381 z 28.12.2006).
- Z dniem 9 kwietnia 2013 r. art. 94 utracił moc w kwestiach wchodzących w zakres Traktatu o Unii Europejskiej, zgodnie z art. 68 ust. 1 Decyzji Rady nr 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz.UE L 205 z 7.08.2007).

2. Kategorie danych obejmują następujące pozycje:
   a) osoby, w przypadku których został wprowadzony wpis;
   b) przedmioty określone w artykułach 99 i 100.
3. W przypadku osób, informacje powinny zawierać jedynie następujące dane:
   a) nazwisko i imiona, wszelkie pseudonimy, wprowadzane, o ile to możliwe, oddzielnie;
   b) wszelkie szczególne cechy fizyczne, niepodlegające zmianom;
   c) pierwszą literę drugiego imienia;
   d) miejsce i datę urodzenia;
   e) płeć;
   f) narodowość;
   g) informację, czy dane osoby są uzbrojone, agresywne bądź są uciekinierami;
   h) przyczynę wpisu;
   i) działania, które powinny być podjęte;
   j) w przypadku wpisów na mocy art. 95: rodzaj przestępstw(-a).

   Pozostałe informacje, w szczególności dane wymienione w artykułu 6 zdanie pierwsze Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 lutego 1981 roku, nie są dopuszczone.
4. W przypadku gdy Umawiająca się Strona uzna, że wpis zgodnie z artykułami 95, 97 lub 99 jest niezgodny z jej prawem krajowym, jej zobowiązaniami międzynarodowymi lub podstawowymi interesami narodowymi, może dodać do wpisu zawartego w pliku danych krajowego modułu Systemu Informacyjnego Schengen zastrzeżenie informujące, że działanie podejmowane na podstawie wpisu nie zostanie podjęte na jej terytorium. W tej sprawie konieczne jest przeprowadzenie konsultacji z pozostałymi Umawiającymi się Stronami. Jeśli Umawiająca się Strona wprowadzająca wpis nie wycofa zastrzeżenia, jest on nadal stosowany w odniesieniu do innych Umawiających się Stron.

Artykuł 95

1. Dane na temat osób poszukiwanych do aresztowania ekstradycyjnego są wprowadzane na wniosek władzy sądowej wzywającej Umawiającej się Strony.
2. Do czasu wprowadzenia wpisu, Umawiająca się Strona sprawdzi, czy aresztowanie jest dozwolone na mocy prawa krajowego wezwanej Umawiającej się Strony. Jeśli Umawiająca się Strona wprowadzająca wpis ma jakiekolwiek wątpliwości, powinna zasięgnąć opinii innych zainteresowanych Umawiających się Stron.

   Umawiająca się Strona wprowadzająca wpis przesyła wezwanym Umawiającym się Stronom najszybszymi sposobami zarówno wpis, jak i następujące podstawowe informacje odnoszące się do danej sprawy:
   a) organ, który wydał wniosek o aresztowanie;
   b) informację, czy istnieje nakaz aresztowania lub inny dokument mający

identyczny skutek prawny, lub podlegający wykonaniu wyrok;
c) charakter i kwalifikację prawną przestępstwa;
d) opis okoliczności, w których przestępstwo zostało popełnione, w tym czas, miejsce oraz stopień udziału w przestępstwie osoby, w przypadku której wpis został wprowadzony;
e) tak dalece jak to możliwe, konsekwencje popełnienia przestępstwa.

3. Wezwana Umawiająca się Strona może dodać do pliku danych w swoim krajowym module Systemu Informacyjnego Schengen zastrzeżenie zakazujące aresztowania na podstawie wpisu do czasu usunięcia zastrzeżenia. Zastrzeżenie powinno zostać usunięte nie później niż 24 godziny po wprowadzeniu wpisu, o ile Umawiająca się Strona odmawia dokonania żądanego aresztowania z uwagi na przyczyny prawne lub ze względów praktycznych. W szczególnych sytuacjach, kiedy jest to uzasadnione skomplikowanym charakterem faktów leżących u podstaw wpisu, wyżej wymieniony termin może być przedłużony do jednego tygodnia. Bez uszczerbku dla wprowadzonego zastrzeżenia lub decyzji w sprawie odmowy aresztowania pozostałe Umawiające się Strony mogą dokonać aresztowania żądanego we wpisie.
4. Jeśli ze szczególnie pilnych powodów Umawiająca się Strona zażąda przeprowadzenia natychmiastowej rewizji, wezwana Umawiająca się Strona zbada, czy jest w stanie wycofać wprowadzone zastrzeżenie. Wezwana Umawiająca się Strona podejmie niezbędne kroki w celu zapewnienia, aby działania zostały przeprowadzone niezwłocznie po potwierdzeniu wpisu.
5. Jeśli aresztowanie nie może być dokonane z uwagi na nie zakończenie dochodzenia lub dlatego że wezwana Umawiająca się Strona go odmawia, Strona ta powinna uznać wpis za wpis do celów podania miejsca pobytu danej osoby.
6. Wezwane Umawiające się Strony przeprowadzają działania wymagane we wpisie zgodnie z obowiązującymi konwencjami o ekstradycji oraz prawem krajowym. Nie są one zobowiązane do przeprowadzania żądanych działań, jeśli dotyczą one jednego z jej obywateli, bez uszczerbku dla możliwości aresztowania tej osoby zgodnie z prawem krajowym.

Artykuł 96

1. Dane dotyczące cudzoziemców, w przypadku których został wprowadzony wpis do celów odmowy wjazdu są wprowadzane na podstawie krajowego wpisu wynikającego z decyzji podjętych przez właściwe organy administracyjne lub sądy zgodnie z zasadami proceduralnymi ustanowionymi przez prawo krajowe.
2. Decyzje mogą być uzasadniane zagrożeniem dla porządku publicznego, bezpieczeństwa publicznego lub bezpieczeństwa narodowego, jakie może stwarzać obecność cudzoziemca na terytorium państwowym.

Sytuacja ta może mieć miejsce w szczególności w przypadku:

a) cudzoziemca, który został skazany za przestępstwo zagrożone karą pozbawienia wolności powyżej roku;
b) cudzoziemca, w odniesieniu do którego istnieją poważne podstawy, aby przypuszczać, że popełnił poważne przestępstwa, w tym przestępstwa

określone w artykule 71, lub w odniesieniu do którego istnieje wyraźny dowód zamiaru popełnienia takich przestępstw na terytorium Umawiającej się Strony.

3. Decyzje mogą być również oparte na fakcie, że cudzoziemiec został poddany środkom, obejmującym deportację, odmowę wjazdu lub usunięcie, które nie zostały unieważnione lub zawieszone, w tym zakaz wjazdu lub, tam gdzie to stosowne, zakaz pobytu, z uwagi na niespełnianie przepisów dotyczących wjazdu lub pobytu cudzoziemców.

Artykuł 97

Dane dotyczące osoby lub osób zaginionych, które dla ich własnej ochrony lub w celu zapobiegania zagrożeniom powinny być tymczasowo oddane pod opiekę policji na wniosek właściwego organu lub właściwej władzy sądowej Strony wprowadzającej wpis, powinny zostać wprowadzone, aby organy policyjne mogły poinformować o danych ich dotyczących Stronę wprowadzającą wpis lub przetransportować osobę do bezpiecznego miejsca w celu zapobieżenia kontynuowania jej podróży, o ile jest to dozwolone przez prawo krajowe. Ma to zastosowanie w szczególności do małoletnich lub osób, które powinny zostać internowane w wyniku decyzji podjętej przez właściwy organ. Przekazywanie danych na temat pełnoletnich osób zaginionych zależy od zgody zainteresowanej osoby.

Artykuł 98

1. Dane dotyczące świadków, osób wezwanych do stawienia się przed organami sądowymi w związku z postępowaniem karnym w celu poniesienia odpowiedzialności za czyny, za które są ścigane, lub osób, które powinny odbywać wyrok w sprawie karnej lub wezwanych do stawienia się w celu odbycia kary pozbawienia wolności, wprowadza się na wniosek właściwych organów sądowych, w celach poinformowania o ich miejscu zamieszkania lub pobytu.
2. Żądane informacje zostaną przekazane żądającej Stronie zgodnie z prawem krajowym oraz obowiązującymi konwencjami dotyczącymi wzajemnej pomocy w sprawach karnych.

Artykuł 99

1. Dane dotyczące osób lub pojazdów, łodzi, statków powietrznych i kontenerów są wprowadzane zgodnie z prawem krajowym Państwa Członkowskiego dokonującego wpisu, do celów niejawnego nadzoru lub szczególnych kontroli zgodnie z ust. 5.
2. Wpis taki może zostać wprowadzony w celach ścigania przestępstw oraz zapobiegania zagrożeniom dla bezpieczeństwa publicznego:
   a) jeśli istnieje wyraźny dowód, że dana osoba zamierza popełnić przestępstwo lub popełnia liczne i szczególnie poważne przestępstwa; lub
   b) jeśli ogólna ocena danej osoby, w szczególności na podstawie wcześniej popełnionych przestępstw, daje powód do przypuszczenia, że powyższa

osoba popełni szczególnie poważne przestępstwa w przyszłości.

3. Ponadto wpis może zostać wprowadzony zgodnie z prawem krajowym na wniosek organów odpowiedzialnych za bezpieczeństwo narodowe, jeśli istnieje wyraźny dowód, że informacje określone w ustępie 4 są niezbędne dla zapobiegania poważnym zagrożeniom przez daną osobę lub poważnym zagrożeniom dla wewnętrznego i zewnętrznego bezpieczeństwa narodowego. Państwo Członkowskie dokonujące wpisu zgodnie z niniejszym ustępem jest zobowiązane do powiadomienia o tym pozostałych Państw Członkowskich.
4. Do celów niejawnego nadzoru mogą być zbierane oraz przekazywane organom wprowadzającym wpis w przypadku kontroli granicznej lub innych kontroli policyjnych i celnych przeprowadzanych w ramach danego kraju wszystkie lub niektóre poniższe informacje:
   a) fakt, że stwierdzono obecność osoby, w przypadku której lub w przypadku pojazdu której został wprowadzony wpis;
   b) miejsce, czas lub przyczyny kontroli;
   c) droga oraz cel podróży;
   d) osoby towarzyszące danej osobie lub osoby przewożone pojazdem;
   e) używany pojazd;
   f) przewożone przedmioty;
   g) okoliczności, w których osoba lub pojazd zostały znalezione.

   Podczas zbierania tych informacji należy podjąć kroki w celu zachowania niejawnego charakteru prowadzonego nadzoru.
5. Podczas szczególnych kontroli, określonych w ustępie 1, osoby, pojazdy, łodzie, statki powietrzne i kontenery oraz przewożone przedmioty mogą zostać przeszukane zgodnie z prawem krajowym w celach określonych w ust. 2 i 3. Jeśli szczególna kontrola nie jest dozwolona na mocy przepisów prawnych Umawiającej się Strony, jest ona automatycznie zastępowana w przypadku tej Umawiającej się Strony niejawnym nadzorem.
6. Wezwana Umawiająca się Strona może dodać do wpisu znajdującego się w pliku danych jej krajowego modułu Systemu Informacyjnego Schengen zastrzeżenie zakazujące, do czasu jego usunięcia, prowadzenia działań na podstawie wpisu do celów niejawnego nadzoru lub szczególnych kontroli. Zastrzeżenie powinno zostać usunięte nie później niż 24 godziny po jego wprowadzeniu, jeśli Umawiająca się Strona odmawia podjęcia działania z przyczyn prawnych lub ze szczególnych powodów praktycznych. Bez uszczerbku dla wprowadzenia zastrzeżenia lub odmowy, inne Umawiające się Strony mogą przeprowadzać działania wymagane we wpisie.

Artykuł 100

1. Dane dotyczące przedmiotów niezbędne do celów ich zajęcia lub wykorzystania w charakterze dowodu w postępowaniu karnym powinny zostać wprowadzone do Systemu Informacyjnego Schengen.
2. Jeśli przegląd wyjawi wpis dotyczący przedmiotu, który został znaleziony, organ, który porównał dwie pozycje danych, skontaktuje się z organem, który

wprowadził wpis w celu uzgodnienia środków, które należy podjąć. W tym celu dane osobowe mogą również być przekazywane zgodnie z niniejszą Konwencją. Środki podejmowane przez Umawiającą się Stronę, która znalazła przedmiot, powinny być zgodne z jej prawem krajowym.

3. Wprowadza się następujące kategorie łatwo rozpoznawalnych przedmiotów:
   a) pojazdy silnikowe o pojemności silnika przekraczającej 50 cm^3, łodzie i statki powietrzne, które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone;
   b) przyczepy o masie własnej przekraczającej 750 kg, naczepy, sprzęt przemysłowy, silniki zewnętrzne i kontenery, które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone;
   c) broń palna, która została skradziona, wykorzystana w niewłaściwy sposób lub utracona;
   d) urzędowe blankiety, które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone;
   e) wydane dokumenty tożsamości, takie jak paszporty, dowody tożsamości, prawa jazdy, dokumenty pobytowe i dokumenty podróżne, które zostały skradzione, wykorzystane w niewłaściwy sposób, utracone lub unieważnione;
   f) dowody rejestracyjne pojazdów i tablice rejestracyjne, które zostały skradzione, wykorzystane w niewłaściwy sposób, utracone lub unieważnione;
   g) banknoty (o spisanych numerach);
   h) papiery wartościowe i środki płatnicze, takie jak czeki, karty kredytowe, obligacje, akcje i udziały, które zostały skradzione, wykorzystane w niewłaściwy sposób lub utracone.

Artykuł 101

1. Dostęp do danych wprowadzonych do Systemu Informacyjnego Schengen oraz prawo do ich bezpośredniego przeglądania jest zastrzeżone wyłącznie dla organów odpowiedzialnych za:
   a) kontrole graniczne;
   b) inne kontrole policyjne i celne prowadzone w ramach danego kraju, jak również koordynację takich kontroli.

   Jednak dostęp do danych wprowadzonych do Systemu Informacyjnego Schengen oraz prawo do ich bezpośredniego przeglądania mogą mieć krajowe organy sądowe, między innymi organy odpowiedzialne za wszczynanie postępowania karnego z oskarżenia publicznego oraz wszczynanie dochodzenia sądowego poprzedzającego postawienie w stan oskarżenia, podczas wykonywania swoich funkcji, zgodnie z przepisami prawa krajowego.
2. Ponadto, dostęp do danych wprowadzonych zgodnie z artykułem 96 i danych dotyczących dokumentów odnoszących się do osób wprowadzonych do systemu zgodnie z art. 100 ust. 3 lit. d) i e) oraz prawo dokonywania bezpośredniego przeszukania tych danych może być wykonywane przez organy odpowiedzialne za wydawanie wiz, władze centralne odpowiedzialne za rozpa-

trywanie wniosków wizowych oraz organy odpowiedzialne za wydawanie pozwoleń na pobyt stały oraz za administrację przepisów prawnych dotyczących cudzoziemców w kontekście stosowania postanowień niniejszej Konwencji w odniesieniu do przepływu osób. Dostęp tych organów do tych danych jest regulowany w przepisach krajowych każdego Państwa Członkowskiego.
3. Użytkownicy mogą przeglądać tylko te dane, które są im potrzebne do wykonywania ich zadań.
4. Każda z Umawiających się Stron przekazuje Komitetowi Wykonawczemu wykaz właściwych władz, które są upoważnione do bezpośredniego przeglądania danych zawartych w Systemie Informacyjnym Schengen. Powyższy wykaz powinien wskazywać, w odniesieniu do każdego organu, które dane mogą przeglądać i do jakich celów.

Artykuł 101A
1. Europejski Urząd Policji (Europol) ma prawo dostępu i bezpośredniego przeglądania danych wprowadzonych do Systemu Informacyjnego Schengen, w ramach swojego mandatu i na własny koszt, zgodnie z artykułami 95, 99 i 100.
2. Europol może przeglądać tylko te dane, które są mu potrzebne do wykonywania swoich zadań.
3. W przypadku gdy podczas przeglądania danych Europol odkryje istnienie wpisu w Systemie Informacyjnym Schengen, informuje o tym, przy wykorzystaniu środków określonych w Konwencji o Europolu, Państwo Członkowskie, które dokonało wpisu.
4. Korzystanie z informacji uzyskanych poprzez przeglądanie danych Systemu Informacyjnego Schengen wymaga zgody zainteresowanego Państwa Członkowskiego.

   Jeżeli to Państwo Członkowskie pozwoli na wykorzystanie takich informacji, procedura taka odbywa się zgodnie z postanowieniami Konwencji o Europolu. Europol może przekazać takie informacje państwom trzecim i organom trzecim wyłącznie po uzyskaniu zgody zainteresowanego Państwa Członkowskiego.
5. Europol może zażądać informacji uzupełniających od zainteresowanego Państwa Członkowskiego zgodnie z postanowieniami Konwencji o Europolu.
6. Europol:
   a) prowadzi ewidencję wszystkich wykonanych przez siebie wyszukiwań, zgodnie z postanowieniami artykułu 103;
   b) bez uszczerbku dla ustępów 4 i 5, nie łączy części Systemu Informacyjnego Schengen ani nie przekazuje udostępnianych im danych w nim zawartych przy użyciu jakiegokolwiek systemu komputerowego wykorzystywanego przez Europol lub stosowanego w Europolu służącego do gromadzenia i przetwarzania danych, ani nie pobiera lub w inny sposób nie kopiuje jakiejkolwiek części Systemu Informacyjnego Schengen;
   c) zapewnia dostęp do danych wprowadzonych do Systemu Informacyjnego Schengen wyłącznie pracownikom Europolu o specjalnych uprawnie-

niach;
d) przyjmuje i stosuje środki przewidziane w artykule 118;
e) zezwala wspólnemu organowi nadzorczemu, ustanowionemu na mocy artykułu 24 Konwencji o Europolu, na przeprowadzenie kontroli działalności Europolu w wykonaniu jego prawa do dostępu i przeglądania danych wprowadzonych do Systemu Informacyjnego Schengen.

Artykuł 101B

1. Krajowi przedstawiciele Eurojustu i ich asystenci mają prawo dostępu i przeglądania danych wprowadzonych do Systemu Informacyjnego Schengen zgodnie z artykułami 95 i 98.
2. Krajowi przedstawiciele Eurojustu i ich asystenci mogą przeglądać jedynie te dane, które są niezbędne do wykonywania ich zadań.
3. W przypadku gdy podczas przeglądania danych krajowy przedstawiciel Eurojustu odkryje istnienie wpisu w Systemie Informacyjnym Schengen, informuje o tym Państwo Członkowskie, które dokonało wpisu. Informacje uzyskane w wyniku takiego wyszukiwania mogą być przekazywane państwom trzecim i organom trzecim po otrzymaniu zgody Państwa Członkowskiego, które dokonało wpisu.
4. Żadnego postanowienia niniejszego artykułu nie należy rozumieć jako naruszającego przepisy decyzji Rady ustanawiającej Eurojust dotyczące ochrony danych i odpowiedzialności za wszelkie nieuprawnione lub niepoprawne przetwarzanie takich danych przez krajowych przedstawicieli Eurojustu lub ich asystentów lub jako naruszające uprawnienia wspólnego organu nadzorczego, ustanowionego zgodnie z artykułem 23 tej decyzji Rady.
5. Każde wyszukiwanie przeprowadzone przez krajowego przedstawiciela Eurojustu lub asystenta zostaje wpisane do ewidencji zgodnie z postanowieniami artykułu 103, a każde wykorzystanie udostępnionych im danych jest rejestrowane.
6. Żadnych części Systemu Informacyjnego Schengen nie należy łączyć, a danych zawartych w tym systemie dostępnych krajowym przedstawicielom i ich asystentom nie należy przekazywać do żadnego systemu komputerowego wykorzystywanego przez Eurojust lub stosowanego w Eurojuście służącego do gromadzenia i przetwarzania danych, ani nie należy pobierać jakiejkolwiek części Systemu Informacyjnego Schengen.
7. Dostęp do danych wprowadzonych do Systemu Informacyjnego Schengen mają wyłącznie przedstawiciele krajowi i ich asystenci, a nie pracownicy Eurojustu.
8. Środki przewidziane w artykule 118 zostają przyjęte i są stosowane. Środki przewidziane w artykule 118 zostają przyjęte i są stosowane.

ROZDZIAŁ 3

OCHRONA DANYCH OSOBOWYCH ORAZ BEZPIECZEŃSTWO DANYCH

W SYSTEMIE INFORMACYJNYM SCHENGEN

Artykuł 102

1. Umawiające się Strony mogą wykorzystywać dane określone w artykułach 95-100 wyłącznie do celów ustanowionych dla każdej kategorii wpisów określonych w powyższych artykułach.
2. Dane mogą być kopiowane wyłącznie do celów technicznych, pod warunkiem że takie kopiowanie jest niezbędne w celu przeprowadzenia bezpośredniego przeglądu przez organy określone w artykule 101. Wpisy wprowadzane przez inne Umawiające się Strony nie mogą być kopiowane z krajowych modułów Systemu Informacyjnego Schengen do innych krajowych plików danych.
3. W odniesieniu do wpisów określonych w artykułach 95–100 niniejszej Konwencji, wszelkie odstępstwo od ustępu 1 w celu zmiany z jednej kategorii wpisu na inną powinno być uzasadnione potrzebą zapobiegania bezpośredniemu poważnemu zagrożeniu dla porządku publicznego oraz bezpieczeństwa publicznego, z poważnych przyczyn bezpieczeństwa narodowego lub do celów zapobiegania popełnieniu poważnych przestępstw. W tym celu należy uzyskać uprzednie upoważnienie od Umawiającej się Strony wprowadzającej wpis.
4. Dane nie mogą być wykorzystywane do celów administracyjnych. W drodze odstępstwa, dane wprowadzone na mocy art. 96 oraz dane dotyczące dokumentów odnoszących się do osób wprowadzonych do systemu na mocy art. 100 ust. 3 lit. d) i e) mogą być wykorzystywane zgodnie z prawem krajowym każdego z Państw Członkowskich wyłącznie do celów art. 101 ust. 2.
5. Wszelkie wykorzystanie danych, które nie jest zgodne z ustępami 1–4, uznaje się za niewłaściwe wykorzystanie zgodnie z prawem krajowym każdej z Umawiających się Stron.

Artykuł 103

Każde Państwo Członkowskie zapewnia, aby każde przekazanie danych osobowych zostało zarejestrowane w krajowym module Systemu Informacyjnego Schengen przez administratora pliku danych organu w celach sprawdzenia, czy przeglądanie danych jest dozwolone, czy nie.

Wpis do rejestru może być wykorzystywany wyłącznie do tego celu i zostaje on usunięty możliwie szybko po upływie jednego roku a najpóźniej po upływie trzech lat.

Artykuł 104

1. Wpisy są regulowane prawem krajowym Umawiającej się Strony wprowadzającej wpis, o ile niniejsza Konwencja nie ustanawia bardziej rygorystycznych warunków.
2. W przypadku gdy niniejsza Konwencja nie ustanawia postanowień szczególnych, do danych wprowadzanych do krajowych modułów Systemu Informacyjnego Schengen stosuje się przepisy prawne każdej z Umawiających się Stron.

3. W przypadku gdy niniejsza Konwencja nie ustanawia postanowień szczególnych dotyczących wykonywania działań żądanych we wpisie, stosuje się prawo krajowe wykonującej działania wezwanej Umawiającej się Strony. W przypadku gdy niniejsza Konwencja ustanawia postanowienia szczególne dotyczące wykonywania działań żądanych we wpisie, odpowiedzialność za powyższe działania jest regulowana prawem krajowym wezwanej Umawiającej się Strony. Jeśli żądane działania nie mogą być przeprowadzone, wezwana Umawiająca się Strona niezwłocznie informuje o powyższym Umawiającą się Stronę wprowadzającą wpis.

Artykuł 105
Umawiająca się Strona wprowadzająca wpis odpowiada za zapewnienie, aby dane wprowadzane do Systemu Informacyjnego Schengen były prawdziwe, aktualne i zgodne z prawem.

Artykuł 106
1. Jedynie Umawiająca się Strona wprowadzająca wpis jest upoważniona do modyfikowania, uzupełniania, korekty lub usuwania wprowadzanych danych.
2. Jeśli jedna z Umawiających się Stron, która nie wprowadziła wpisu, posiada dowody sugerujące, że pozycja w danych jest faktycznie nieścisła lub jest przechowywana z naruszeniem przepisów prawnych, poinformuje ona o powyższym Umawiającą się Stronę wprowadzającą wpis; ta ostatnia jest zobowiązana do sprawdzenia informacji oraz, jeśli to konieczne, do niezwłocznego skorygowania lub usunięcia powyższej pozycji.
3. Jeśli Umawiające się Strony nie są w stanie osiągnąć porozumienia, Umawiająca się Strona, która nie wprowadziła wpisu, przekazuje sprawę do wspólnego organu nadzorczego, określonego w artykule 115 ustęp 1, w celu uzyskania jego opinii.

Artykuł 107
Jeśli dana osoba już podlega wpisowi w Systemie Informacyjnym Schengen, Umawiająca się Strona, która wprowadza kolejny wpis, powinna porozumieć się w sprawie wprowadzenia wpisu z Umawiającą się Stroną, która wprowadziła wpis jako pierwsza. Umawiające się Strony mogą również ustanowić postanowienia ogólne w tym celu.

Artykuł 108
1. Każda z Umawiających się Stron wyznacza organ, odpowiedzialny za jej krajowy moduł Systemu Informacyjnego Schengen.
2. Każda z Umawiających się Stron wprowadza swoje wpisy za pośrednictwem powyższego organu.
3. Wymieniony organ odpowiada za właściwe funkcjonowanie krajowego modułu Systemu Informacyjnego Schengen oraz przyjmuje niezbędne środki

w celu zapewnienia zgodności z postanowieniami niniejszej Konwencji.
4. Umawiające się Strony informują się wzajemnie za pośrednictwem depozytariusza o organach określonych w ustępie 1.

Artykuł 109
1. Prawo osób do dostępu do danych wprowadzanych do Systemu Informacyjnego Schengen ich dotyczących wykonywane jest zgodnie z prawem krajowym Umawiającej się Strony, wobec której powołują się na to prawo. Jeśli prawo krajowe tak stanowi, krajowy organ nadzorczy, określony w artykule 114 ustęp 1, zdecyduje, czy informacje mają być przekazane oraz zgodnie z jakimi procedurami. Umawiająca się Strona, która nie wprowadziła wpisu, może przekazać informację dotyczącą takich danych tylko wtedy, gdy uprzednio dała możliwość Umawiającej się Stronie wprowadzającej wpis wyrażenia swojego stanowiska.
2. Odmawia się przekazywania informacji osobie, której dotyczą dane, jeśli jest to konieczne dla wykonania zgodnego z prawem zadania w związku z wpisem lub dla ochrony praw i swobód stron trzecich. W każdym przypadku odmowa obowiązuje przez okres ważności wpisu wprowadzonego do celów niejawnego nadzoru.

Artykuł 110
Każda osoba może spowodować wprowadzenie korekt do danych faktycznie niedokładnych lub usuniecie danych jej dotyczących przechowywanych z naruszeniem prawa.

Artykuł 111
1. Każda osoba może, na terytorium każdej z Umawiających się Stron, wystąpić do sądów lub organów właściwych na mocy prawa krajowego z żądaniem o dokonanie korekty, usunięcie lub uzyskanie informacji lub uzyskanie odszkodowania w związku z wpisem jej dotyczącym.
2. Umawiające się Strony zobowiązują się do wykonania ostatecznych decyzji podjętych przez sądy lub organy określone w ustępie 1, bez uszczerbku dla postanowień artykułu 116.

Artykuł 112
1. Dane osobowe wprowadzane do Systemu Informacyjnego Schengen do celów śledzenia osób są przechowywane jedynie przez okres konieczny dla osiągnięcia celów, dla których zostały dostarczone. Umawiająca się Strona, która wprowadziła wpis, dokona przeglądu potrzeby ciągłego gromadzenia takich danych najpóźniej w trzy lata od ich wprowadzenia. Okres ten wynosi rok w przypadku wpisów określonych w artykule 99.
2. Każda z Umawiających się Stron, tam gdzie to stosowne, ustanowi krótsze okresy przeglądu zgodnie ze swoim prawem krajowym.

3. Jednostka centralna Systemu Informacyjnego Schengen automatycznie informuje z jednomiesięcznym wyprzedzeniem Umawiające się Strony o zamierzonym usunięciu danych z systemu.
4. Umawiająca się Strona wprowadzająca wpis może w trakcie okresu przeglądu podjąć decyzję o zachowaniu wpisu, o ile jest to konieczne do celów, dla których wpis został wprowadzony. Przedłużenie wpisu powinno być odnotowane w jednostce centralnej. Do przedłużonego wpisu stosuje się postanowienia ustępu 1.

Artykuł 112A
1. Dane osobowe przechowywane przez władze, określone w artykule 92 ustęp 4 otrzymane w wyniku wymiany informacji zgodnie z tym ustępem, są przechowywane jedynie przez okres wymagany do osiągnięcia celów, dla których zostały one dostarczone. W każdym przypadku należy je usunąć najpóźniej po roku od momentu, gdy wpis lub wpisy dotyczące danej osoby lub przedmiotu zostały usunięte z Systemu Informacyjnego Schengen.
2. Ustęp 1 nie narusza prawa Państw Członkowskich do przechowywania krajowych danych dotyczących poszczególnych wpisów, które zostały wprowadzone przez dane Państwo Członkowskie lub wpisów, w związku z którymi podjęto działania na terytorium tego państwa. Okres przechowywania takich danych określa prawo krajowe.

Artykuł 113
1. Dane inne niż określone w artykule 112 są przechowywane przez okres nie dłuższy niż 10 lat a dane dotyczące przedmiotów określonych w artykule 99 ustęp 1 przez okres nie dłuższy niż 5 lat.
2. Dane, które zostały skreślone, są przechowywane przez okres jednego roku w jednostce centralnej. W tym okresie mogą być one tylko konsultowane dla dalszej weryfikacji ich dokładności oraz tego, czy dane te zostały wprowadzone legalnie. Po upływie powyższego okresu dane powinny zostać zniszczone.

Artykuł 113 A
1. Dane inne niż dane osobowe przechowywane przez władze określone w artykule 92 ustęp 4 otrzymane w wyniku wymiany informacji zgodnie z tym ustępem, są przechowywane jedynie przez okres wymagany do osiągnięcia celów, dla których zostały one przekazane.

   W każdym przypadku należy je usunąć najpóźniej po roku od momentu, gdy wpis lub wpisy dotyczące danej osoby lub przedmiotu zostały usunięte z Systemu Informacyjnego Schengen.
2. Ustęp 1 nie narusza prawa Państw Członkowskich do przechowywania krajowych danych dotyczących poszczególnych wpisów, które zostały wprowadzone przez dane Państwo Członkowskie, lub wpisów, w związku z którymi podjęto działania na terytorium tego państwa. Okres przechowywania takich danych określa prawo krajowe.

Artykuł 114
1. Każda z Umawiających się Stron wyznacza organ nadzorczy odpowiedzialny, zgodnie z prawem krajowym, za przeprowadzanie niezależnego nadzoru nad danymi krajowego modułu Systemu Informacyjnego Schengen oraz za kontrolę, czy przetwarzanie i wykorzystywanie danych wprowadzanych do Systemu Informacyjnego Schengen nie narusza praw osób, których dane te dotyczą. W tym celu organ nadzorczy ma dostęp do plików danych w krajowym module Systemu Informacyjnego Schengen.
2. Każda osoba ma prawo poprosić organy nadzorcze o sprawdzenie danych wprowadzonych do Systemu Informacyjnego Schengen, które jej dotyczą, oraz sposobu ich wykorzystania. Prawo powyższe jest regulowane prawem krajowym Umawiającej się Strony, do której wniosek taki jest kierowany. Jeśli dane zostały wprowadzone przez inną Umawiającą się Stronę, sprawdzenie jest przeprowadzane w ścisłej koordynacji z organem nadzorczym tej Umawiającej się Strony.

Artykuł 115
1. Tworzy się wspólny organ nadzorczy, który jest odpowiedzialny za nadzór nad jednostką centralną Systemu Informacyjnego Schengen. Organ ten składa się z dwóch przedstawicieli każdego krajowego organu nadzorczego. Każda z Umawiających się Stron ma jeden głos. Nadzór jest prowadzony zgodnie z postanowieniami niniejszej Konwencji, Konwencji Rady Europy z dnia 28 stycznia 1981 roku o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, uwzględniając zalecenie Komitetu Ministrów Rady Europy nr R (87) 15 z dnia 17 września 1987 roku regulujące wykorzystywanie danych osobowych w sektorze policji, oraz zgodnie z prawem krajowym Umawiającej się Strony odpowiedzialnej za jednostkę centralną.
2. W odniesieniu do jednostki centralnej Systemu Informacyjnego Schengen, zadaniem wspólnego organu nadzorczego jest sprawdzanie, czy postanowienia niniejszej Konwencji są właściwie wykonywane. W tym celu organ ten posiada dostęp do jednostki centralnej.
3. Wspólny organ nadzorczy odpowiada również za rozpatrywanie wszelkich trudności związanych ze stosowaniem lub wykładnią, jakie mogą się pojawić w związku z funkcjonowaniem Systemu Informacyjnego Schengen, za badanie wszelkich problemów, jakie mogą się pojawić w związku z wykonywaniem niezależnego nadzoru przez krajowe organy nadzorcze Umawiających się Stron lub z wykonywaniem prawa dostępu do systemu, oraz za przygotowywanie zharmonizowanych propozycji wspólnych rozwiązań napotkanych problemów.
4. Sprawozdania przygotowywane przez wspólny organ nadzorczy są przekazywane organom, do których krajowe organy nadzorcze przekazują swoje sprawozdania.

Artykuł 116

1. Każda z Umawiających się Stron ponosi odpowiedzialność, zgodnie ze swoim prawem krajowym, za wszelkie szkody wyrządzone osobom poprzez wykorzystanie krajowych danych Systemu Informacyjnego Schengen. Stosuje się to również do szkód wyrządzonych przez Umawiającą się Stronę, która wprowadziła wpis, jeśli Strona ta wprowadziła faktycznie dane niedokładne lub przechowuje dane nielegalnie.
2. Jeśli Umawiająca się Strona, przeciwko której- wniesione zostało powództwo, nie jest Umawiającą się Stroną wprowadzającą wpis, ta ostatnia jest zobowiązana do zwrotu, na wniosek tej pierwszej, sum zapłaconych w charakterze odszkodowania, jeśli dane zostały wykorzystane przez wezwaną Umawiającą się Stronę z naruszeniem niniejszej Konwencji.

Artykuł 117

1. W odniesieniu do automatycznego przetwarzania danych osobowych przekazywanych na mocy niniejszego tytułu, każda z Umawiających się Stron, nie później niż w momencie wejścia w życie niniejszej Konwencji, przyjmie niezbędne przepisy krajowe w celu osiągnięcia poziomu ochrony danych osobowych, co najmniej równego temu wynikającemu z zasad ustanowionych w Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 roku oraz zgodnie z zaleceniem Komitetu Ministrów Rady Europy nr R (87) 15 z dnia 17 września 1987 roku regulującym wykorzystywanie danych osobowych w sektorze policji.
2. Przekazywanie danych osobowych przewidzianych w niniejszym tytule nie może mieć miejsca do czasu wejścia w życie na terytoriach Umawiających się Stron uczestniczących w przekazywaniu danych postanowień dotyczących ochrony danych osobowych określonych w ustępie 1.

Artykuł 118

1. Każda z Umawiających się Stron zobowiązuje się, w odniesieniu do swojego krajowego modułu Systemu Informacyjnego Schengen, przyjąć niezbędne środki w celu:
   a) odmowy nieupoważnionym osobom dostępu do sprzętu służącego do przetwarzania danych osobowych (kontrola dostępu do sprzętu);
   b) zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji lub usuwaniu nośników danych (kontrola nośników danych);
   c) zapobiegania nieupoważnionemu wprowadzaniu danych oraz nieupoważnionym inspekcjom, modyfikacjom lub usuwaniu przechowywanych danych osobowych (kontrola gromadzenia danych);
   d) zapobiegania wykorzystywania zautomatyzowanych systemów przetwarzania danych przez nieupoważnione osoby z wykorzystaniem sprzętu do przekazywania danych (kontrola użytkownika);
   e) zapewnienia, aby osoby upoważnione do wykorzystywania zautomatyzo-

wanych systemów przetwarzania danych miały jedynie dostęp do danych objętych ich upoważnieniem (kontrola dostępu do danych);

f) zapewnienia możliwości weryfikacji i stwierdzania, do których organów dane osobowe mogą być przekazywane z wykorzystaniem sprzętu do przekazywania danych (kontrola transmisji danych);

g) zapewnienia możliwości weryfikacji i stwierdzenia, które dane osobowe zostały wprowadzone do zautomatyzowanych systemów przetwarzania danych, oraz kiedy i przez kogo dane zostały wprowadzone (kontrola dostarczania danych);

h) zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji lub usuwaniu danych osobowych podczas przekazywania danych osobowych lub podczas przenoszenia nośników danych (kontrola dostarczania danych).

2. Każda z Umawiających się Stron powinna przyjąć specjalne środki dla zapewnienia bezpieczeństwa danych podczas ich przekazywania służbom znajdującym się poza terytoriami Umawiających się Stron. Środki takie powinny być notyfikowane wspólnemu organowi nadzorczemu.
3. Do celów przetwarzania danych w swoim krajowym module Systemu Informacyjnego Schengen, każda z Umawiających się Stron może wyznaczyć tylko osoby o szczególnie wysokich kwalifikacjach, w stosunku do których przeprowadzono kontrolę bezpieczeństwa.
4. Umawiająca się Strona odpowiedzialna za jednostkę centralną Systemu Informacyjnego Schengen przyjmie środki ustanowione w ustępach 1–3 w odniesieniu do powyższej funkcji.

ROZDZIAŁ 4

PODZIAŁ KOSZTÓW SYSTEMU INFORMACYJNEGO SCHENGEN

Artykuł 119

1. Koszty instalacji i eksploatacji jednostki centralnej, o której mowa w art. 92 ust. 3, w tym koszty okablowania łączącego krajowe moduły Systemu Informacyjnego Schengen z jednostką centralną oraz koszty działań podejmowanych w związku z zadaniami powierzonymi Francji na mocy decyzji 2008/839/WSiSW oraz rozporządzenia (WE) nr 1104/2008 ponoszą wspólnie Państwa Członkowskie.

   Udział każdej z Umawiających się Stron zostanie określony na podstawie udziału dla każdej z Umawiających się Stron stosowanego do jednolitej podstawy naliczenia podatku od wartości dodanej w rozumieniu artykułu 2 ustęp 1 litera c) decyzji Rady Wspólnot Europejskich z dnia 24 czerwca 1988 roku w sprawie systemu środków własnych Wspólnot.
2. Koszty instalacji i eksploatacji krajowego modułu Systemu Informacyjnego Schengen oraz koszty zadań przydzielonych krajowym systemom na mocy decyzji 2008/839/WSiSW oraz rozporządzenia (WE) nr 1104/2008 są ponoszone indywidualnie przez każde Państwo Członkowskie.

Aneks 2[7]

USTAWA
z dnia 24 sierpnia 2007 r.
o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej
(Dz.U. z 2007 r. Nr 165, poz. 1170)

ROZDZIAŁ 1
PRZEPISY OGÓLNE

Art. 1. Ustawa określa zasady i tryb udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, w tym obowiązki organów dokonujących wpisów oraz organów uprawnionych do dostępu do danych w zakresie wykorzystywania informacji zawartych w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej poprzez Krajowy System Informatyczny (KSI).

Art. 2. Ilekroć w ustawie jest mowa o:

1) bezpośrednim dostępie – rozumie się przez to dostęp do danych wykorzystywanych poprzez Krajowy System Informatyczny, realizowany w sposób bezpośredni przez organ wskazany w ustawie;
2) Centralnym Systemie Informacji Wizowej – rozumie się przez to Centralny Wizowy System Informacyjny, o którym mowa w art. 1 ust. 2 decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (Dz. Urz. UE L 213 z 15.06.2004, str. 5–7);
3) centralnym organie technicznym KSI – rozumie się przez to Komendanta Głównego Policji;
4) danych – rozumie się przez to dane SIS lub dane VIS;
5) danych SIS – rozumie się przez to dane określone w art. 94 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. UE L 239 z 22.09.2000, str. 19, z późn. zm.), zwanej dalej „Konwencją Wykonawczą";
6) danych VIS – rozumie się przez to dane przetwarzane w Systemie Informacji Wizowej, określone w odrębnych przepisach wydanych przez organy Unii Europejskiej, dotyczących funkcjonowania Systemu Informacji Wizowej;
7) informacjach uzupełniających – rozumie się przez to wszelkie informacje, wymieniane za pośrednictwem biur SIRENE między krajowymi a zagranicznymi organami uprawnionymi do wykorzystywania danych SIS, niezbędne przy dokonywaniu wpisów do Systemu Informacyjnego Schengen lub w celu umożliwienia podjęcia odpowiednich działań, w przypadkach gdy w wyniku przeglądania danych SIS odnaleziono osoby lub przedmioty, których dotyczą wpisy;

[7] Interpunkcja w tekście zgodna z oryginałem.

8) interfejsie krajowym – rozumie się przez to interfejs krajowy, o którym mowa w art. 1 ust. 2 decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego;
9) jednostce centralnej Systemu Informacyjnego Schengen – rozumie się przez to jednostkę centralną Systemu Informacyjnego Schengen, o której mowa w art. 92 ust. 3 Konwencji Wykonawczej;
10) kopii krajowej – rozumie się przez to kopię bazy danych SIS z jednostki centralnej Systemu Informacyjnego Schengen;
11) Krajowym Systemie Informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, oprogramowania, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych oraz infrastrukturę telekomunikacyjną, umożliwiające organom administracji publicznej i organom wymiaru sprawiedliwości przekazywanie oraz dostęp do danych gromadzonych w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej;
12) module krajowym – rozumie się przez to polski krajowy moduł Systemu Informacyjnego Schengen, o którym mowa w art. 92 ust. 2 Konwencji Wykonawczej;
13) Państwie Członkowskim – rozumie się przez to państwo członkowskie Unii Europejskiej, państwo członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym nienależące do Unii Europejskiej lub państwo niebędące stroną umowy o Europejskim Obszarze Gospodarczym, którego obywatele mogą korzystać ze swobody przepływu osób na podstawie umów zawartych przez to państwo ze Wspólnotą Europejską i jej państwami członkowskimi, z wyjątkiem państwa, wobec którego Rada podjęła decyzję o niestosowaniu przepisów dorobku Schengen;
14) pośrednim dostępie – rozumie się przez to dostęp do danych wykorzystywanych poprzez Krajowy System Informatyczny, realizowany w sytuacjach wskazanych w ustawie za pośrednictwem centralnego organu technicznego KSI albo organu wskazanego w art. 7 ust. 2;
15) Systemie Informacyjnym Schengen – rozumie się przez to system informacyjny, o którym mowa w art. 92 ust. 1–3 Konwencji Wykonawczej;
16) Systemie Informacji Wizowej – rozumie się przez to system, o którym mowa w art. 1 decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego;
17) wpisie – rozumie się przez to czynności faktyczne skutkujące wprowadzeniem do Systemu Informacyjnego Schengen lub Systemu Informacji Wizowej zestawu danych umożliwiających właściwym organom identyfikację osoby lub przedmiotu oraz podjęcie wnioskowanego działania w związku ze zidentyfikowaniem osoby lub przedmiotu;
18) wykorzystywaniu danych – rozumie się przez to przetwarzanie danych będących danymi osobowymi w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883 z późn. zm., t.j.

Dz.U. z 2015 r. poz. 2135, 2281, z 2016 r. poz. 195[1]), jak również jakiekolwiek operacje wykonywane na danych niebędących danymi osobowymi, takie jak zbieranie, wpisywanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

ROZDZIAŁ 2

ORGANY I SŁUŻBY UPRAWNIONEDO WYKORZYSTYWANIA DANYCH

Art. 3.1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych SIS dotyczących:

1) osób poszukiwanych do tymczasowego aresztowania w celu wydania ich na wniosek państw obcych przysługuje sądowi lub prokuraturze;
2) osób poszukiwanych do tymczasowego aresztowania w celu przekazania osoby ściganej na podstawie europejskiego nakazu aresztowania przysługuje sądowi lub prokuraturze;
3) świadków lub osób wezwanych do stawienia się przed sądami w związku z postępowaniem karnym w celu poniesienia odpowiedzialności za czyny, za które są ścigane, lub osób, wobec których powinien zostać wykonany wyrok w sprawie karnej, lub osób wezwanych do stawienia się w celu odbycia kary pozbawienia wolności, dla ustalenia miejsca ich pobytu przysługuje sądowi lub prokuraturze;
4) cudzoziemców, o których mowa w art. 134a ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach (Dz.U. z 2006 r. Nr 234, poz. 1694 oraz z 2007 r. Nr 120, poz. 818 i Nr 165, poz. 1170), przysługuje Szefowi Urzędu do Spraw Cudzoziemców;
5) osób zaginionych lub osób, które dla ich ochrony lub w celu zapobiegania stwarzanym przez nie zagrożeniom powinny zostać oddane do właściwej placówki opiekuńczej lub leczniczej, przysługuje Policji;
6) osób zaginionych, których miejsce przebywania należy ustalić, przysługuje Policji;
7) osób lub pojazdów, statków wodnych, statków powietrznych i kontenerów, wprowadzonych w celu:
   a) przeprowadzania niejawnego nadzorowania, którego celem jest ściganie przestępstw oraz zapobieganie zagrożeniom bezpieczeństwa publicznego, przysługuje Policji, organom kontroli skarbowej lub Straży Granicznej,
   b) przeprowadzania kontroli, której celem jest ściganie przestępstw oraz zapobieganie zagrożeniom bezpieczeństwa publicznego, przysługuje Policji, organom kontroli skarbowej, Straży Granicznej lub Służbie Celnej,
   c) przeprowadzania niejawnego nadzorowania, którego celem jest zapobieganie poważnym zagrożeniom wewnętrznego i zewnętrznego bezpieczeństwa państwa, przysługuje Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego lub Służbie Wywiadu Wojskowego,
   d) przeprowadzania kontroli, której celem jest zapobieganie poważnym zagrożeniom wewnętrznego i zewnętrznego bezpieczeństwa państwa,

przysługuje Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego lub Służbie Wywiadu Wojskowego;

e) przedmiotów do celów ich zajęcia lub wykorzystania jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym przysługuje sądowi, prokuraturze, Policji, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Centralnemu Biuru Antykorupcyjnemu, organom kontroli skarbowej lub Służbie Celnej.

2. W przypadku braku bezpośredniego dostępu do Krajowego Systemu Informatycznego spowodowanego przyczynami niezależnymi od danego organu, organy wymienione w ust. 1 mogą dokonywać wpisów danych SIS za pośrednictwem centralnego organu technicznego KSI.

Art. 4.1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu wglądu do danych SIS dotyczących:

1) osób poszukiwanych do tymczasowego aresztowania w celu wydania ich na wniosek państw obcych przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celnej, organom kontroli skarbowej, sądowi lub prokuraturze;
2) osób poszukiwanych do tymczasowego aresztowania w celu przekazania osoby ściganej na podstawie europejskiego nakazu aresztowania przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celnej, organom kontroli skarbowej, sądowi lub prokuraturze;
3) świadków lub osób wezwanych do stawienia się przed sądami w związku z postępowaniem karnym w celu poniesienia odpowiedzialności za czyny, za które są ścigane, lub osób, wobec których powinien zostać wykonany wyrok w sprawie karnej, lub osób wezwanych do stawienia się w celu odbycia kary pozbawienia wolności, dla ustalenia miejsca ich pobytu przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celnej, organom kontroli skarbowej, sądowi lub prokuraturze;
4) cudzoziemców, których dane zostały wpisane do Systemu Informacyjnego Schengen dla celów odmowy wjazdu, o których mowa w art. 134a ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach, przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Agencji Wywiadu, Służbie Celnej, organom kontroli skarbowej, sądowi, prokuraturze, Szefowi Urzędu do Spraw Cudzoziemców, Służbie Kontrwywiadu Wojskowego, wojewodzie, konsulowi lub ministrowi właściwemu do spraw zagranicznych;
5) osób zaginionych lub osób, które dla ich ochrony lub w celu zapobiegania stwarzanym przez nie zagrożeniom powinny zostać oddane do właściwej placówki opiekuńczej lub leczniczej, przysługuje Straży Granicznej, Służbie Celnej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej,

Centralnemu Biuru Antykorupcyjnemu, organom kontroli skarbowej, sądowi lub prokuraturze;

6) osób zaginionych, których miejsce przebywania należy ustalić, przysługuje Straży Granicznej, Służbie Celnej, Policji, Agencji Bezpieczeństwa Wewnętrznego lub Żandarmerii Wojskowej;
7) osób lub pojazdów, statków wodnych, statków powietrznych i kontenerów, wprowadzonych w celu przeprowadzania niejawnego nadzorowania lub kontroli przysługuje Straży Granicznej, Służbie Celnej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Służbie Kontrwywiadu Wojskowego, Centralnemu Biuru Antykorupcyjnemu, organom kontroli skarbowej, sądowi lub prokuraturze;
8) przedmiotów w celu ich zajęcia lub wykorzystania jako dowód w postępowaniu karnym, wskazanych w art. 100 ust. 3 Konwencji Wykonawczej, przysługuje Straży Granicznej, Służbie Celnej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, organom kontroli skarbowej, ministrowi właściwemu do spraw wewnętrznych, sądowi lub prokuraturze;
9) przedmiotów w celu ich zajęcia lub wykorzystania jako dowód w postępowaniu karnym, wskazanych w art. 100 ust. 3 lit. d i e Konwencji Wykonawczej, przysługuje wojewodzie, konsulowi lub Szefowi Urzędu do Spraw Cudzoziemców;
10) przedmiotów w celu ich zajęcia lub wykorzystania jako dowód w postępowaniu karnym, wskazanych w art. 100 ust. 3 lit. a, b i f Konwencji Wykonawczej, przysługuje Biuru Ochrony Rządu, Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Służbie Kontrwywiadu Wojskowego, organom jednostek wojskowych Sił Zbrojnych Rzeczypospolitej Polskiej, Centralnemu Biuru Antykorupcyjnemu, Straży Granicznej, organom kontroli skarbowej, Służbie Celnej lub wojewodzie mazowieckiemu.

2. Uprawnienie do pośredniego dostępu do Krajowego Systemu Informatycznego w celu wglądu do danych SIS dotyczących przedmiotów do celów ich zajęcia lub wykorzystania jako dowód w postępowaniu karnym, wskazanych w art. 100 ust. 3 lit. a, b i f Konwencji Wykonawczej, przysługuje organom samorządowym właściwym w sprawach rejestracji pojazdów.

3. Uprawnienie do wglądu do danych SIS przysługuje organom określonym w ust. 1 pkt 10 i ust. 2 wyłącznie w związku z wykonywaniem obowiązku rejestracji pojazdów określonego w art. 73 i 74 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. z 2005 r. Nr 108, poz. 908, z późn. zm.[2)]) w celu sprawdzenia, czy zgłoszone do rejestracji pojazdy nie zostały skradzione, przywłaszczone lub utracone w inny sposób.

4. Organy, o których mowa w ust. 1 i 2, w przypadku odnalezienia na skutek wglądu do danych SIS osoby lub przedmiotu, których dotyczy wpis, są obowiązane do podjęcia wnioskowanych we wpisie działań, o ile realizowane przez dany organ zadania umożliwiają im takie działania, albo do bezzwłocznego przekazania osoby lub przedmiotu Policji.

5. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb przekazywania Policji osób lub przedmiotów odnalezionych na skutek wglądu do danych SIS, a także związane z tym obowiązki Policji, uwzględniając sprawną i skuteczną realizację wnioskowanych we wpisie działań wobec odnalezionych osób lub przedmiotów.

Art. 5.1. Bezpośredni dostęp do Systemu Informacji Wizowej realizowany jest poprzez Krajowy System Informatyczny w celu dokonywania, zmieniania lub usuwania wpisów danych VIS przez Straż Graniczną, konsula, wojewodę, ministra właściwego do spraw zagranicznych, Szefa Urzędu do Spraw Cudzoziemców lub Policję.

2. Organy określone w ust. 1 są obowiązane do:

1) wymiany krajowych danych VIS poprzez dokonywanie wpisów do Centralnego Systemu Informacji Wizowej poprzez Krajowy System Informatyczny;
2) zapewnienia, aby dokonywane przez dany organ wpisy danych VIS były zgodne z prawem, a ponadto, aby te dane VIS były dokładne i aktualne;
3) zapewnienia usuwania dokonanych przez dany organ wpisów danych VIS po upływie okresu, na który wpisy te zostały wprowadzone;
4) niezwłocznego informowania centralnego organu technicznego KSI o ujawnionych nieprawidłowościach w związku z wykorzystaniem danych VIS poprzez Krajowy System Informatyczny;
5) rozpatrywania wniosków Państw Członkowskich o uaktualnienie, uzupełnienie, skorygowanie lub wykasowanie wprowadzonego przez dany organ wpisu danych VIS.

Art. 6. Bezpośredni dostęp do Systemu Informacji Wizowej realizowany poprzez Krajowy System Informatyczny umożliwiający wgląd do danych VIS:

1) w celu rozpatrzenia wniosków wizowych oraz zbadania podjętych decyzji dotyczących tych wniosków, zgodnie z odpowiednimi postanowieniami Wspólnych Instrukcji Konsularnych, przysługuje Straży Granicznej, konsulowi, wojewodzie, ministrowi właściwemu do spraw zagranicznych, Szefowi Urzędu do Spraw Cudzoziemców lub Policji;
2) w celu przeprowadzania konsultacji, o których mowa w art. 17 ust. 2 Konwencji Wykonawczej, przysługuje Szefowi Urzędu do Spraw Cudzoziemców;
3) w celach sprawozdawczych i statystycznych przysługuje Straży Granicznej, konsulowi, wojewodzie, ministrowi właściwemu do spraw zagranicznych, Szefowi Urzędu do Spraw Cudzoziemców lub Policji;
4) w celu przeprowadzania kontroli wiz na granicach i na terytorium Rzeczypospolitej Polskiej, wyłącznie w celu potwierdzenia tożsamości osoby lub potwierdzenia autentyczności wizy, przysługuje Straży Granicznej, Policji, Służbie Celnej lub Szefowi Urzędu do Spraw Cudzoziemców;
4) w celu weryfikacji dla ustalenia, czy warunki wjazdu i pobytu są spełnione, przysługuje komendantowi wojewódzkiemu Policji, komendantowi powiatowemu (miejskiemu) Policji, komendantowi oddziału Straży Granicznej lub

komendantowi placówki Straży Granicznej, wojewodzie lub Szefowi Urzędu do Spraw Cudzoziemców;
6) w celu określania odpowiedzialności Państwa Członkowskiego za rozpatrywanie wniosków o nadanie statusu uchodźcy w rozumieniu rozporządzenia Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiającego kryteria i mechanizmy określania Państwa Członkowskiego, które jest odpowiedzialne za rozpatrzenie wniosku o azyl złożonego w jednym z Państw Członkowskich przez obywatela kraju trzeciego (Dz. Urz. UE L 050 z 25.02.2003, str. 1; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 19, t. 6, str. 109), przysługuje Szefowi Urzędu do Spraw Cudzoziemców;
7) w celu rozpatrywania wniosku o nadanie statusu uchodźcy przysługuje Szefowi Urzędu do Spraw Cudzoziemców lub Radzie do Spraw Uchodźców.

Art. 7.1. Uprawnienie do pośredniego dostępu do Krajowego Systemu Informatycznego w celu wglądu do danych VIS przysługuje sądowi, prokuraturze, Policji, Straży Granicznej, Służbie Celnej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, organom kontroli skarbowej, Biuru Ochrony Rządu, Służbie Kontrwywiadu Wojskowego, Żandarmerii Wojskowej lub Służbie Wywiadu Wojskowego, jeżeli:
1) dostęp jest konieczny w celu zapobiegania, wykrywania lub ścigania przestępstw wymienionych w art. 607w ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. Nr 89, poz. 555, z późn. zm.[3)]);
2) jest to niezbędne w związku z określoną sprawą;
3) istnieją uzasadnione powody do uznania, że wgląd do danych VIS ma istotne znaczenie dla zapobiegania, wykrywania lub ścigania przestępstw, o których mowa w pkt 1.

2. Pośredni dostęp, o którym mowa w ust. 1, jest realizowany poprzez centralne punkty dostępu, którymi są odpowiednio dla:
1) sądu, prokuratury, Policji – Komendant Główny Policji;
2) Straży Granicznej – Komendant Główny Straży Granicznej;
3) Służby Celnej – Szef Służby Celnej;
4) Agencji Bezpieczeństwa Wewnętrznego – Szef Agencji Bezpieczeństwa Wewnętrznego;
5) Agencji Wywiadu – Szef Agencji Wywiadu;
6) Centralnego Biura Antykorupcyjnego – Szef Centralnego Biura Antykorupcyjnego;
7) organów kontroli skarbowej – Generalny Inspektor Kontroli Skarbowej;
8) Biura Ochrony Rządu – Szef Biura Ochrony Rządu;
9) Służby Kontrwywiadu Wojskowego – Szef Służby Kontrwywiadu Wojskowego;
10) Służby Wywiadu Wojskowego – Szef Służby Wywiadu Wojskowego;
11) Żandarmerii Wojskowej – Komendant Główny Żandarmerii Wojskowej.

ROZDZIAŁ 3

OCHRONA DANYCH OSOBOWYCH ORAZ ODPOWIEDZIALNOŚĆ ZA NIEZGODNE Z PRAWEM DZIAŁANIE LUB ZANIECHANIE ZWIĄZANE Z WYKORZYSTYWANIEM DANYCH

Art. 8.1. Generalny Inspektor Ochrony Danych Osobowych sprawuje kontrolę nad tym, czy wykorzystywanie danych nie narusza praw osób, których dane te dotyczą.

2. Generalny Inspektor Ochrony Danych Osobowych jest uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu sprawowania kontroli, o której mowa w ust. 1.

3. Kontrola, o której mowa w ust. 1, jest sprawowana zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Art. 9. Generalny Inspektor Ochrony Danych Osobowych, w przypadku, o którym mowa w art. 106 ust. 3 Konwencji Wykonawczej, jest organem uprawnionym do przekazania sprawy wspólnemu organowi nadzorczemu wskazanemu w art. 115 ust. 1 Konwencji Wykonawczej, w celu uzyskania jego opinii.

Art. 10. Centralny organ techniczny KSI, w zakresie wykorzystywania danych poprzez Krajowy System Informatyczny, jest administratorem danych w rozumieniu art. 7 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Art. 11. Wykorzystywanie danych może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez obowiązku ujawniania faktycznego celu zbierania danych.

Art. 12. W sprawie o naprawienie szkody wyrządzonej przez niezgodne z prawem działanie lub zaniechanie związane z wykorzystywaniem danych SIS organem reprezentującym Skarb Państwa jest Prokuratoria Generalna Skarbu Państwa.

Art. 13. W sprawie o naprawienie szkody wyrządzonej przez niezgodne z prawem działanie lub zaniechanie związane z wykorzystywaniem danych VIS organem reprezentującym Skarb Państwa jest organ, w związku z działaniem lub zaniechaniem którego szkoda ta powstała, z zastrzeżeniem art. 8 ustawy z dnia 8 lipca 2005 r. o Prokuratorii Generalnej Skarbu Państwa (Dz.U. Nr 169, poz. 1417, z późn. zm.[4)]).

ROZDZIAŁ 4

BEZPIECZEŃSTWO KRAJOWEGO SYSTEMU INFORMATYCZNEGO

Art. 14. Organy, o których mowa w rozdziale 2, obowiązane są, w zakresie swojego działania, do współpracy z centralnym organem technicznym KSI w celu realizacji ich zadań związanych z udziałem w Systemie Informacyjnym Schengen lub Systemie Informacji Wizowej, w tym do przekazywania dokumentów oraz udzielania informacji.

Art. 15. Centralny organ techniczny KSI składa ministrowi właściwemu do spraw wewnętrznych raz w roku, w terminie do dnia 31 marca, sprawozdanie z funkcjonowania Krajowego Systemu Informatycznego w poprzednim roku kalendarzowym.

Art. 16.1. Minister właściwy do spraw wewnętrznych sprawuje nadzór nad prawidłowością działania Krajowego Systemu Informatycznego.

2. Minister właściwy do spraw wewnętrznych, w celu wykonania nadzoru wynikającego z ust. 1, ma w szczególności prawo:

1) dostępu do wykazu zarejestrowanych przypadków, o których mowa w art. 27 ust. 1 pkt 10;
2) sprawdzania, czy Krajowy System Informatyczny spełnia wymagania techniczne niezbędne do udziału w Systemie Informacyjnym Schengen i Systemie Informacji Wizowej;
3) sprawdzania, czy osoby mające dostęp do Krajowego Systemu Informatycznego zostały odpowiednio przeszkolone w zakresie bezpieczeństwa danych oraz zasad ich ochrony oraz czy posiadają upoważnienie, o którym mowa w art. 25 ust. 2, a także czy wobec tych osób przeprowadzono kontrolę bezpieczeństwa;
4) sprawdzania prawidłowości opisu zadań i funkcji osób mających dostęp do Krajowego Systemu Informatycznego;
5) sprawdzania, czy jest zapewniona odpowiednia fizyczna ochrona Krajowego Systemu Informatycznego przez organy mające do niego bezpośredni dostęp, w szczególności czy nie ma możliwości dostępu osób nieuprawnionych do Krajowego Systemu Informatycznego.

Art. 17.1. Minister właściwy do spraw wewnętrznych, przed uruchomieniem Krajowego Systemu Informatycznego, jest uprawniony do sprawdzenia gotowości do prawidłowej eksploatacji Krajowego Systemu Informatycznego w ramach poszczególnych organów uprawnionych do bezpośredniego dostępu.

2. W przypadku stwierdzenia braku gotowości do prawidłowej eksploatacji Krajowego Systemu Informatycznego w ramach poszczególnych organów uprawnionych do bezpośredniego dostępu minister właściwy do spraw wewnętrznych jest uprawniony do wstrzymania uruchomienia Krajowego Systemu Informatycznego w ramach organu, w przypadku którego stwierdzono nieprawidłowości.

Art. 18. W przypadku stwierdzenia nieprawidłowości działania Krajowego Systemu Informatycznego lub jego zabezpieczenia w poszczególnych organach mających do niego bezpośredni dostęp minister właściwy do spraw wewnętrznych jest uprawniony do zablokowania bezpośredniego dostępu do Krajowego Systemu Informatycznego dla organu, w przypadku którego stwierdzone zostały te nieprawidłowości, do czasu ich usunięcia.

Art. 19. W celu wykonania zadań, o których mowa w art. 16–18, minister właściwy do spraw wewnętrznych może:
1) żądać przedłożenia informacji w zakresie niezbędnym do ustalenia stanu faktycznego;
2) przeprowadzać, w godzinach urzędowania danego organu, oględziny urządzeń, nośników oraz systemów informatycznych włączonych do Krajowego Systemu Informatycznego w ramach danego organu;
3) zlecać sporządzanie ekspertyz i opinii;
4) żądać zablokowania bezpośredniego dostępu do Krajowego Systemu Informatycznego do czasu usunięcia stwierdzonych nieprawidłowości.

Art. 20. W przypadku stwierdzenia nieprawidłowości działania Krajowego Systemu Informatycznego minister właściwy do spraw wewnętrznych może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień i poinformowania tych osób, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

Art. 21.1. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, techniczne warunki, sposób i tryb dokonywania wpisów danych SIS, a także związane z tym obowiązki uprawnionych organów oraz sposób i tryb aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny, mając na względzie prawidłowe wykonywanie przez Rzeczpospolitą Polską zobowiązań wynikających z udziału w Systemie Informacyjnym Schengen.

2. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób wykorzystywania Krajowego Systemu Informatycznego jako krajowego interfejsu Systemu Informacji Wizowej, w tym sposób dokonywania, zmieniania i usuwania wpisów danych VIS, a także wglądu do danych VIS, mając na względzie prawidłowe wykonanie przez Rzeczpospolitą Polską zobowiązań wynikających z udziału w Systemie Informacji Wizowej.

Art. 22.1. Organy uprawnione zgodnie z art. 3 ust. 2 do dokonania wpisu danych SIS za pośrednictwem centralnego organu technicznego KSI kierują wniosek o dokonanie wnioskowanego wpisu danych SIS na wypełnionej karcie wpisu. Centralny organ techniczny KSI niezwłocznie dokonuje wpisu danych SIS, informując o tym organ, który wystąpił z takim wnioskiem, albo informuje organ o braku możliwości dokonania danego wpisu danych SIS oraz jego przyczynach.

2. Organy wskazane w art. 4 ust. 2 kierują zapytanie o dane SIS, do których mają dostęp pośredni, do centralnego organu technicznego KSI na wypełnionej karcie zapytania. Centralny organ techniczny KSI przekazuje niezwłocznie odpowiednie dane SIS organowi składającemu zapytanie.

3. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wzór karty wpisu, o której mowa w ust. 1, oraz wzór karty zapytania,

o której mowa w ust. 2, a także sposób ich wypełnienia, uwzględniając zakres uprawnień organów do wykorzystywania danych SIS.

Art. 23.1. W przypadku stwierdzenia przez organ, który dokonał wpisu danych SIS, że zawarte we wpisie dane SIS są nieprawidłowe, organ ten niezwłocznie dokonuje niezbędnej modyfikacji tych danych, zawiadamiając jednocześnie o tym fakcie centralny organ techniczny KSI.

2. W przypadku stwierdzenia przez organ, który dokonał wpisu danych SIS, że upłynął okres konieczny do osiągnięcia celów, dla których wpis został dokonany albo brak jest podstaw prawnych do dalszego przechowywania tych danych, organ ten usuwa dane SIS, zawiadamiając jednocześnie o tym fakcie centralny organ techniczny KSI.

3. Centralny organ techniczny KSI informuje organy, które zgłosiły zapytanie o dane SIS, o dokonanej modyfikacji danych SIS.

4. Organy, o których mowa w art. 3 i 4, w przypadku stwierdzenia, że wykorzystywane przez te organy dane SIS są nieprawidłowe, niezwłocznie informują o tym Biuro SIRENE w celu weryfikacji prawidłowości tych danych SIS.

Art. 24. Organ uprawniony do wykorzystywania danych poprzez Krajowy System Informatyczny jest obowiązany stosować odpowiednie procedury kontrolne wskazujące działania podejmowane w ramach danego organu mające na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami.

Art. 25.1. Organ uprawniony do wykorzystywania danych poprzez Krajowy System Informatyczny jest obowiązany do przeszkolenia z zakresu bezpieczeństwa i ochrony danych wszystkich osób mających dostęp do Krajowego Systemu Informatycznego.

2. Odbycie szkolenia, o którym mowa w ust. 1, jest warunkiem otrzymania upoważnienia do dostępu do Krajowego Systemu Informatycznego oraz wykorzystywania danych.

3. Minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii Generalnego Inspektora Ochrony Danych Osobowych określi, w drodze rozporządzenia, sposób przeprowadzania szkoleń z zakresu bezpieczeństwa i ochrony danych wykorzystywanych poprzez Krajowy System Informatyczny oraz kwalifikacje osób uprawnionych do przeprowadzania tych szkoleń, uwzględniając konieczność zapewnienia ochrony danych.

4. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb dostępu do Krajowego Systemu Informatycznego, sposób przydzielania osobom upoważnionym do dostępu osobistych i niepowtarzalnych identyfikatorów użytkownika, a także wzór upoważnienia do dostępu do Krajowego Systemu Informatycznego oraz wykorzystywania danych, uwzględniając prawidłową realizację przez Rzeczpospolitą Polską obowiązków wynikających z udziału w Systemie Informacyjnym Schengen.

ROZDZIAŁ 5
CENTRALNY ORGAN TECHNICZNY KSI

Art. 26.1. Organem odpowiedzialnym za moduł krajowy jest centralny organ techniczny KSI.

2. Do zadań centralnego organu technicznego KSI należy:

1) utworzenie, uruchomienie, eksploatacja techniczna oraz utrzymanie Krajowego Systemu Informatycznego;
2) zapewnienie sprawnego działania i bezpieczeństwa Systemu Informacyjnego Schengen w ramach modułu krajowego.

Art. 27.1. W celu realizacji zadań, o których mowa w art. 26 ust. 2 pkt 1, centralny organ techniczny KSI jest w szczególności obowiązany do:

1) przestrzegania obowiązujących protokołów i procedur technicznych w celu zapewnienia kompatybilności Krajowego Systemu Informatycznego z jednostką centralną Systemu Informacyjnego Schengen oraz Centralnym Systemem Informacji Wizowej;
2) zapewnienia, aby dane SIS przechowywane w kopii krajowej były, dzięki automatycznym aktualizacjom, identyczne i spójne z danymi przechowywanymi w jednostce centralnej Systemu Informacyjnego Schengen;
3) zapewnienia bezpieczeństwa Krajowego Systemu Informatycznego, w szczególności poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej;
4) sprawdzania, czy organy, które wykorzystują dane poprzez Krajowy System Informatyczny, mają prawo dostępu do danych;
5) umożliwienia organom, o których mowa w art. 5–7, wykorzystywania danych VIS poprzez Krajowy System Informatyczny oraz udzielania tym organom niezbędnych informacji do prawidłowego wykonywania przez te organy zadań w zakresie uczestnictwa w Systemie Informacji Wizowej;
6) przekazywania Komisji Europejskiej listy organów, o których mowa w art. 5–7;
7) współpracy z Krajowym Oddziałem Europolu w zakresie udzielenia zgody na dostęp Europejskiego Biura Policji Europol do danych VIS;
8) zapobiegania dostępowi osób nieuprawnionych do Krajowego Systemu Informatycznego;
9) zapobiegania nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników informatycznych wykorzystywanych w Krajowym Systemie Informatycznym;
10) zapewnienia rejestrowania wszystkich przypadków, w których uzyskano dostęp do danych lub wykorzystano dane w inny sposób poprzez Krajowy System Informatyczny;
11) zapewnienia fizycznej ochrony danych wykorzystywanych poprzez Krajowy System Informatyczny;
12) zapobiegania wykorzystywaniu systemów informatycznego przetwarzania danych przez osoby nieuprawnione korzystające ze sprzętu do przekazywania danych;

13) zapewnienia możliwości późniejszej weryfikacji i stwierdzenia, które dane zostały wprowadzone poprzez Krajowy System Informatyczny oraz kiedy, przez kogo i w jakim celu dane te zostały wykorzystane;
14) zapobiegania nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych podczas transferu tych danych lub podczas przemieszczania nośników informatycznych w ramach Krajowego Systemu Informatycznego, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania;
15) zapewnienia, aby osoby uprawnione do korzystania z systemu informatycznego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadanym przez te osoby upoważnieniem, poprzez przydzielenie im osobistych i niepowtarzalnych identyfikatorów użytkownika oraz poufny tryb dostępu.

2. W celu realizacji zadań, o których mowa w art. 26 ust. 2 pkt 2, centralny organ techniczny KSI jest w szczególności obowiązany do:
1) umożliwienia organom, o których mowa w art. 3 i 4, wykorzystywania danych SIS poprzez Krajowy System Informatyczny;
2) udzielania informacji niezbędnych do prawidłowego wykonywania zadań przez organy, o których mowa w art. 3 i 4;
3) współdziałania z organami, które są uprawnione do dokonywania wpisów danych SIS poprzez Krajowy System Informatyczny, w celu zapewnienia, aby wpisy danych SIS były zgodne z prawem oraz aby były one dokładne i aktualne;
4) sprawdzania, czy organy, które wykorzystują dane SIS poprzez Krajowy System Informatyczny, mają prawo dostępu do danych SIS;
5) sprawdzenia skuteczności środków mających na celu zapewnienie bezpieczeństwa danych SIS wykorzystywanych poprzez Krajowy System Informatyczny;
6) zapewnienia usuwania danych SIS wprowadzonych poprzez Krajowy System Informatyczny po upływie okresu, na który wpisy te zostały wprowadzone;
8) sprawdzenia zasadności przedłużenia okresu przechowywania danych SIS wprowadzonych poprzez Krajowy System Informatyczny;
8) przekazywania organowi zarządzającemu jednostką centralną Systemu Informacyjnego Schengen wykazu organów, o których mowa w art. 3 i 4;
9) zapobiegania nieuprawnionemu wykorzystywaniu danych SIS.

Art. 28. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, szczegółowy sposób rejestrowania przypadków, o których mowa w art. 27 ust. 1 pkt 10, mając na względzie bezpieczeństwo i ochronę danych wykorzystywanych poprzez Krajowy System Informatyczny.

Art. 29.1. Centralny organ techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego, jest obowiązany poinformować ministra właściwego do spraw wewnętrznych o gotowości Krajowego Systemu Informatycznego do uruchomienia.

2. Minister właściwy do spraw wewnętrznych, po uzyskaniu informacji, o której mowa w ust. 1, przeprowadza kontrolę w zakresie spełniania przez Kra-

jowy System Informatyczny wymogów określonych w art. 92 ust. 2 Konwencji Wykonawczej.

3. Po przeprowadzeniu kontroli, o której mowa w ust. 2, minister właściwy do spraw wewnętrznych przedstawia centralnemu organowi technicznemu KSI pisemną opinię w zakresie spełnienia przez Krajowy System Informatyczny wymogów określonych w art. 92 ust. 2 Konwencji Wykonawczej, a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej.

Art. 30.1. Centralny organ techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego, jest obowiązany do wystąpienia do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o przeprowadzenie kontroli w zakresie spełniania przez Krajowy System Informatyczny wymogów określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz w przepisach wydanych na podstawie art. 39a tej ustawy.

2. Wniosek, o którym mowa w ust. 1, powinien zawierać opis środków technicznych i organizacyjnych określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, wydanych na podstawie art. 39a tej ustawy.

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

4. W celu wykonania zadań, o których mowa w ust. 1, Generalny Inspektor Ochrony Danych Osobowych, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych, 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 Krajowy System Informatyczny i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych;
2) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii;
4) przeprowadzania oględzin poszczególnych elementów Krajowego Systemu Informatycznego, w tym urządzeń, oprogramowania, procedur przetwarzania informacji;
5) zlecać sporządzanie ekspertyz i opinii.

5. Generalny Inspektor Ochrony Danych Osobowych po przeprowadzeniu kontroli, o której mowa w ust. 1, przedstawia centralnemu organowi technicznemu KSI pisemną opinię w zakresie spełnienia przez Krajowy System Informatyczny wymogów określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, a także w przepisach wydanych na podstawie

art. 39a tej ustawy, a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej.

Art. 31.1. W przypadku przedstawienia przez ministra właściwego do spraw wewnętrznych lub Generalnego Inspektora Ochrony Danych Osobowych zaleceń pokontrolnych, centralny organ techniczny KSI ma prawo zgłoszenia na piśmie umotywowanych zastrzeżeń co do przekazanych zaleceń pokontrolnych, w terminie 7 dni od dnia otrzymania zaleceń pokontrolnych.

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

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

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

Art. 33. Uruchomienie Krajowego Systemu Informatycznego może nastąpić pod warunkiem uzyskania pozytywnych opinii, o których mowa w art. 29 ust. 3, art. 30 ust. 5 lub w art. 31 ust. 2 pkt 3.

Art. 34. W przypadku dokonywania jakichkolwiek zmian w Krajowym Systemie Informatycznym po jego uruchomieniu centralny organ techniczny KSI jest obowiązany przed wdrożeniem tych zmian do uzyskania opinii ministra właściwego do spraw wewnętrznych oraz Generalnego Inspektora Ochrony Danych Osobowych, w zakresie i w trybie określonym w art. 29–32.

ROZDZIAŁ 6
BIURO SIRENE

Art. 35.1. W ramach struktury Komendy Głównej Policji tworzy się wyodrębnione organizacyjnie Biuro SIRENE, zapewniające w szczególności wymianę informacji uzupełniających w trybie i zgodnie z zasadami określonymi w Załączniku Nr 1 do Decyzji Komisji 2006758/WE z dnia 22 września 2006 r. w sprawie zmiany podręcznika SIRENE (Dz. Urz. WE L 317 z 16.11.2006, str. 41).

2. Biuro SIRENE, w celu realizacji zadań, posiada bezpośredni dostęp do Krajowego Systemu Informatycznego.

Art. 36. Szefa Biura SIRENE powołuje i odwołuje Komendant Główny Policji po uzyskaniu zgody ministra właściwego do spraw wewnętrznych.

Art. 37.1. Organy, o których mowa w rozdziale 2, są obowiązane, w zakresie swojego działania, do współpracy z Biurem SIRENE w celu realizacji jego zadań związanych z udziałem w Systemie Informacyjnym Schengen, w tym do wymiany informacji uzupełniających.

2. Obowiązek, o którym mowa w ust. 1, dotyczy w szczególności bezzwłocznego przekazywania do Biura SIRENE, w związku z dokonaniem poprzez Krajowy System Informatyczny wpisu danych SIS, kopii decyzji będących podstawą wpisu danych SIS do celów odmowy wjazdu dotyczących cudzoziemców będących członkami rodzin obywateli UE w rozumieniu art. 2 pkt 4 ustawy z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin (Dz.U. Nr 144, poz. 1043 oraz z 2007 r. Nr 120, poz. 818).

ROZDZIAŁ 7
ZMIANY W PRZEPISACH OBOWIĄZUJĄCYCH

Art. 38. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2007 r. Nr 43, poz. 277, Nr 57, poz. 390, Nr 120, poz. 818 i Nr 140, poz. 981) w art. 1 w ust. 2 uchyla się pkt 11.

Art. 39. W ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z 2016 r. poz. 195.[5]) w art. 43 w ust. 1 po pkt 2a dodaje się pkt 2b w brzmieniu: „2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej".

Art. 40. W ustawie z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz o Krajowym Systemie Informatycznym (Dz.U. z 2006 r. Nr 216, poz. 1585 i Nr 220, poz. 1600 oraz z 2007 r. Nr 120, poz. 818) wprowadza się następujące zmiany:

1) tytuł ustawy otrzymuje brzmienie: „Ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych";
2) w art. 4 uchyla się pkt 8;
3) uchyla się rozdział 4a;
4) uchyla się art. 40a i 40b.

Art. 41. W ustawie z dnia 13 czerwca 2003 r. o cudzoziemcach (Dz.U. z 2006 r. Nr 234, poz. 1694 oraz z 2007 r. Nr 120, poz. 818) wprowadza się następujące zmiany:

1) w art. 3 w pkt 2 lit. a otrzymuje brzmienie: „a) art. 93, art. 94, art. 96, art. 100, rozdziałów 9 i 10, art. 124 pkt 1 lit. g oraz pkt 2 i 4, art. 125 ust. 1 pkt 2 w zakresie dotyczącym art. 124 pkt 1 lit. g, art. 126 ust. 1 pkt 4 i 7 oraz ust. 2, art. 127, art. 128 ust. 2, art. 131–134a, które mają zastosowanie do obywateli państw członkowskich Unii Europejskiej, państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stron umowy o Europejskim Obszarze Gospodarczym lub Konfederacji Szwajcarskiej oraz członków ich rodzin,";
2) w art. 4: a) pkt 5 otrzymuje brzmienie:

„5) wiza – zezwolenie wydane cudzoziemcowi przez organ polski lub organ, którego właściwość w tej sprawie wynika z postanowień umów międzynarodowych obowiązujących Rzeczpospolitą Polską lub organ państw obszaru Schengen, uprawniające go do wjazdu na terytorium Rzeczypospolitej Polskiej lub innych państw obszaru Schengen, przejazdu przez to terytorium i pobytu na nim w czasie, w celu i na warunkach w nim określonych;",

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

„5a) wiza jednolita – wiza, o której mowa w art. 10 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. UE L 239 z 22.09.2000, str. 19, z późn. zm.);

5b) wiza krajowa – wiza uprawniająca do wjazdu na terytorium Rzeczypospolitej Polskiej, przejazdu przez to terytorium i pobytu na nim;

5c) centralny organ wizowy – organ odpowiedzialny za przeprowadzenie konsultacji, w tym konsultacji elektronicznych, o których mowa w art. 17 ust. 2 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach;

5d) państwa obszaru Schengen – państwa, które w pełni stosują dorobek Schengen;";

3) art. 28 otrzymuje brzmienie:

„Art. 28. 1. Wiza tranzytowa uprawnia do przejazdu przez terytorium Rzeczypospolitej Polskiej lub innych państw obszaru Schengen i może być wydana cudzoziemcowi, który posiada prawo wjazdu do państwa docelowego lub państwa graniczącego z terytorium Rzeczypospolitej Polskiej.

2. Wizę, o której mowa w ust. 1, wydaje się na okres pobytu nie dłuższy niż 5 dni, licząc od dnia każdego wjazdu na terytorium państw obszaru Schengen.";

4) art. 31 otrzymuje brzmienie:

„Art. 31. 1. Wizę pobytową wydaje się jako wizę jednolitą lub krajową.

2. Wiza pobytowa jednolita uprawnia do wjazdu i nieprzerwanego pobytu na terytorium państw obszaru Schengen lub kilku pobytów następujących po sobie, trwających przez okres nieprzekraczający łącznie 3 miesięcy w okresie 6 miesięcy liczonych od dnia pierwszego wjazdu na to terytorium.

3. Wiza pobytowa krajowa uprawnia do wjazdu i nieprzerwanego pobytu na terytorium Rzeczypospolitej Polskiej lub kilku pobytów następujących po sobie, trwających przez okres nieprzekraczający łącznie roku w okresie ważności wizy.

4. Wiza pobytowa krajowa może być wydana w celu wjazdu i pobytu, o którym mowa w art. 26 pkt 4 lit. b i d–j oraz r, jeżeli okoliczności tego pobytu wymagają, aby trwał on dłużej niż 3 miesiące.

5. Okres pobytu na podstawie wizy pobytowej krajowej ustala się w granicach określonych w ust. 3 i 4 odpowiednio do celu wskazanego przez cudzoziemca.

6. Okres ważności wizy pobytowej może wynosić do 5 lat.";

5) w art. 32 ust. 1 otrzymuje brzmienie:

„1. Wiza pobytowa krajowa w celu wykonywania pracy może być wydana cudzoziemcowi, który przedstawi przyrzeczenie wydania zezwolenia na pracę na terytorium Rzeczypospolitej Polskiej albo pisemne oświadczenie pracodawcy o zamiarze powierzenia cudzoziemcowi wykonywania pracy, jeżeli zezwolenie na pracę nie jest wymagane.";

6) w art. 33 w ust. 1 zdanie wstępne otrzymuje brzmienie:

„Cudzoziemcowi może być wydana wiza pobytowa krajowa, choćby zachodziły okoliczności, o których mowa w art. 42, jeżeli:";

7) w art. 34 ust. 1 otrzymuje brzmienie:

„1. Wizę pobytową krajową wydaje się małoletniemu cudzoziemcowi urodzonemu na terytorium Rzeczypospolitej Polskiej, na wniosek jego przedstawiciela ustawowego, który przebywa na terytorium Rzeczypospolitej Polskiej na podstawie wizy.";

8) w art. 35 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Wizę dyplomatyczną, służbową i kurierską wydaje się jako wizę krajową.";

9) w art. 42 zdanie wstępne otrzymuje brzmienie:

„Cudzoziemcowi odmawia się wydania wizy krajowej, jeżeli:",

10) po art. 42 dodaje się art. 42a w brzmieniu:

„Art. 42a. Cudzoziemcowi odmawia się wydania wizy pobytowej jednolitej, jeżeli jego dane znajdują się w wykazie cudzoziemców, których pobyt na terytorium Rzeczypospolitej Polskiej jest niepożądany, lub w przypadku gdy cudzoziemiec nie spełnia warunków wjazdu, o których mowa w art. 5 ust. 1 lit. a, c, d i e rozporządzenia (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. ustanawiającego wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz. Urz. UE L 105 z 13.04.2006, str. 1).";

11) w art. 44 ust. 1 otrzymuje brzmienie:

„1. Cudzoziemiec jest obowiązany złożyć wniosek o przedłużenie wizy co najmniej 7 dni przed upływem okresu pobytu oznaczonego w posiadanej wizie jednolitej lub co najmniej 14 dni przed upływem okresu pobytu oznaczonego w posiadanej wizie krajowej.";

12) po art. 45 dodaje się art. 45a i 45b w brzmieniu:

„Art. 45a. 1. Wydanie wizy jednolitej w przypadkach określonych przez Radę Unii Europejskiej na podstawie art. 17 ust. 2 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach wymaga uzyskania zgody Szefa Urzędu do Spraw Cudzoziemców działającego jako centralny organ wizowy.

2. Szef Urzędu do Spraw Cudzoziemców konsultuje możliwość wyrażenia zgody na wydanie wizy jednolitej:

1) w przypadkach określonych w załączniku 5A do Wspólnych Instrukcji Konsularnych dla misji dyplomatycznych i urzędów konsularnych dotyczących wiz (Dz. Urz. UE C 326 z 22.12.2005, str. 1), zwanych dalej „Wspólnymi Instrukcjami Konsularnymi", z:

a) Komendantem Głównym Straży Granicznej,

b) Komendantem Głównym Policji,

c) Szefem Agencji Bezpieczeństwa Wewnętrznego,

d) Szefem Agencji Wywiadu,

e) ministrem właściwym do spraw zagranicznych;

2) w przypadkach określonych w załączniku 5B do Wspólnych Instrukcji Konsularnych z centralnymi organami wizowymi innych państw obszaru Schengen.

3. Jeżeli wydanie wizy jednolitej przez organ wizowy innego państwa obszaru Schengen wymaga zgody centralnego organu wizowego Rzeczypospolitej Polskiej, Szef Urzędu do Spraw Cudzoziemców działający jako centralny organ wizowy konsultuje możliwość wyrażenia zgody z organami, o których mowa w ust. 2 pkt 1.

4. Organy, o których mowa w ust. 2 pkt 1, są obowiązane, w terminie 5 dni od dnia otrzymania wniosku o konsultację, przekazać opinię w sprawie zgody na wydanie wizy jednolitej. Nieprzekazanie opinii w tym terminie uznaje się za równoważne z wydaniem opinii pozytywnej.

5. Na wniosek organów, o których mowa w ust. 2 pkt 1, termin przekazania opinii w sprawie zgody na wydanie wizy jednolitej może być przedłużony o 5 dni, a w szczególnie uzasadnionych przypadkach do 80 dni, o czym Szef Urzędu do Spraw Cudzoziemców zawiadamia konsula.

6. Szef Urzędu do Spraw Cudzoziemców informuje konsula o wyrażeniu zgody na wydanie wizy jednolitej lub braku zgody na jej wydanie, w terminie 10 dni od dnia otrzymania wniosku w tej sprawie. Termin ten ulega przedłużeniu odpowiednio do przedłużenia terminu przekazania opinii w sprawie zgody na wydanie wizy jednolitej, o którym mowa w ust. 5.

7. Nieudzielenie konsulowi przez Szefa Urzędu do Spraw Cudzoziemców informacji w sprawie zgody na wydanie wizy jednolitej w terminach, o których mowa w ust. 6, uznaje się za wyrażenie zgody.

8. W przypadku gdy brak zgody na wydanie wizy jednolitej wynika ze stanowiska centralnego organu wizowego innego państwa obszaru Schengen, konsul

może wydać cudzoziemcowi wizę jednolitą upoważniającą tylko do wjazdu na terytorium Rzeczypospolitej Polskiej.

Art. 45b. 1. Przed wydaniem wizy organ właściwy do jej wydania może zwrócić się do Szefa Urzędu do Spraw Cudzoziemców z wnioskiem o przekazanie informacji, czy wobec cudzoziemca zachodzą okoliczności, o których mowa w art. 42 pkt 1–4 i 7.

2. Szef Urzędu do Spraw Cudzoziemców jest obowiązany przekazać informacje, czy wobec cudzoziemca zachodzą okoliczności, o których mowa w art. 42 pkt 1–4 i 7, w terminie 10 dni od dnia otrzymania wniosku w tej sprawie.";

13) w art. 46:

a) ust. 2 otrzymuje brzmienie:

„2. Wizę pobytową krajową w celu wykonywania pracy wydaje lub odmawia jej wydania konsul właściwy ze względu na miejsce stałego zamieszkania cudzoziemca.",

b) uchyla się ust. 7a i 7b;

14) w art. 48 w ust. 1 zdanie wstępne otrzymuje brzmienie:

„Wizę krajową unieważnia się, jeżeli:";

15) w art. 52 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) oznaczenie wiz, z wyłączeniem wiz wydawanych szefom i członkom personelu misji dyplomatycznych, kierownikom urzędów konsularnych i członkom personelu konsularnego państw obcych oraz innym osobom zrównanym z nimi na podstawie ustaw, umów lub powszechnie ustalonych zwyczajów międzynarodowych, i wzór wizy krajowej, uwzględniając jej typy, o których mowa w art. 26, a także zakres danych, które powinny być w niej zawarte, określony w art. 25 ust. 1–4;";

16) w art. 57:

a) w ust. 1 po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) jego dane znajdują się w Systemie Informacyjnym Schengen do celów odmowy wjazdu;",

b) po ust. 5 dodaje się ust. 5a w brzmieniu:

„5a. W przypadku, o którym mowa w ust. 1 pkt 2a, można udzielić zezwolenia na zamieszkanie na czas oznaczony tylko w razie istnienia poważnych przyczyn, zwłaszcza ze względów humanitarnych lub z powodu zobowiązań międzynarodowych, z uwzględnieniem interesu państwa, które dokonało wpisu do Systemu Informacyjnego Schengen.";

17) w art. 62:

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

„7b. W przypadku, o którym mowa w art. 57 ust. 1 pkt 2a, gdy zachodzą okoliczności, o których mowa w art. 57 ust. 5a, wojewoda zasięga opinii, o której mowa w art. 25 ust. 1 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, za pośrednictwem Komendanta Głównego Policji.",

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

„8a. Wojewoda jest obowiązany ustalić, czy zachodzą przesłanki do cofnięcia zezwolenia na zamieszkanie na czas oznaczony, w przypadku gdy państwo obszaru Schengen zasięga opinii na podstawie art. 25 ust. 2 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach.”,

c) w ust. 9 dodaje się pkt 3 w brzmieniu:

„3) właściwy organ państwa obszaru Schengen, za pośrednictwem Komendanta Głównego Policji, o:

a) udzieleniu zezwolenia na zamieszkanie na czas oznaczony w przypadku, o którym mowa w art. 25 ust. 1 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach,

b) braku przesłanek do cofnięcia zezwolenia na zamieszkanie na czas oznaczony w przypadku, o którym mowa w art. 25 ust. 2 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach.”;

18) art. 66 otrzymuje brzmienie:

„Art. 66. 1. Cudzoziemcowi odmawia się udzielenia zezwolenia na osiedlenie się, jeżeli:

1) nie spełnia wymogów, o których mowa w art. 64 ust. 1;

2) jego dane znajdują się w wykazie cudzoziemców, których pobyt na terytorium Rzeczypospolitej Polskiej jest niepożądany;

3) jego dane znajdują się w Systemie Informacyjnym Schengen do celów odmowy wjazdu;

4) wymagają tego względy obronności lub bezpieczeństwa państwa albo ochrony bezpieczeństwa i porządku publicznego lub interes Rzeczypospolitej Polskiej;

5) podstawą ubiegania się o zezwolenie jest zawarcie związku małżeńskiego z obywatelem polskim, a związek małżeński został zawarty wyłącznie w celu obejścia przepisów o udzielaniu zezwolenia na zamieszkanie na czas oznaczony lub zezwolenia na osiedlenie się;

6) w postępowaniu o udzielenie zezwolenia na osiedlenie się:

a) złożył wniosek lub dołączył do niego dokumenty zawierające nieprawdziwe dane osobowe lub fałszywe informacje,

b) zeznał nieprawdę lub zataił prawdę albo, w celu użycia za autentyczny, podrobił lub przerobił dokument bądź takiego dokumentu jako autentycznego używał;

7) nie wywiązuje się z zobowiązań podatkowych wobec Skarbu Państwa.

2. W przypadku, o którym mowa w ust. 1 pkt 3, można udzielić zezwolenia na osiedlenie się tylko w razie istnienia poważnych przyczyn, zwłaszcza ze względów humanitarnych lub z powodu zobowiązań międzynarodowych, z uwzględnieniem interesu państwa, które dokonało wpisu do Systemu Informacyjnego Schengen.";

19) w art. 71b:

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

„6a. W przypadku, o którym mowa w art. 66 ust. 1 pkt 3, gdy zachodzą okoliczności, o których mowa w art. 66 ust. 2, oraz przed wydaniem zezwolenia na pobyt rezydenta długoterminowego WE wojewoda zasięga opinii, o której mowa w art. 25 ust. 1 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, za pośrednictwem Komendanta Głównego Policji.",

b) dodaje się ust. 9 i 10 w brzmieniu:

„9. W przypadku, o którym mowa w art. 25 ust. 1 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, oraz przed wydaniem zezwolenia na pobyt rezydenta długoterminowego WE, wojewoda informuje właściwy organ państwa obszaru Schengen, za pośrednictwem Komendanta Głównego Policji, o wydaniu zezwolenia na osiedlenie się.

10. W przypadku, o którym mowa w art. 25 ust. 2 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, oraz przed wydaniem zezwolenia na pobyt rezydenta długoterminowego WE, wojewoda informuje właściwy organ państwa obszaru Schengen, za pośrednictwem Komendanta Głównego Policji, o braku przesłanek do cofnięcia zezwolenia na osiedlenie się.";

20) w art. 88 w ust. 1 po pkt 4 dodaje się pkt 4a w brzmieniu:

„4a) jego dane znajdują się w Systemie Informacyjnym Schengen do celów odmowy wjazdu, jeżeli cudzoziemiec przebywa na terytorium Rzeczypospolitej Polskiej na podstawie wizy pobytowej krótkoterminowej lub w ruchu bezwizowym;";

21) w art. 128 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) cudzoziemiec został skazany prawomocnym wyrokiem:

a) w Rzeczypospolitej Polskiej za przestępstwo umyślne lub przestępstwo skarbowe na karę grzywny lub karę pozbawienia wolności poniżej jednego roku,

b) w innym państwie niż państwo obszaru Schengen za przestępstwo stanowiące zbrodnię pospolitą również w rozumieniu prawa polskiego,

c) w państwie obszaru Schengen za przestępstwo na karę pozbawienia wolności powyżej jednego roku;";

22) w art. 131:

a) ust. 1 otrzymuje brzmienie:

„1. Cudzoziemiec może złożyć wniosek o:

1) udzielenie informacji o wpisaniu jego danych osobowych do wykazu lub do Systemu Informacyjnego Schengen;

2) sprostowanie jego danych osobowych zawartych w wykazie lub w Systemie Informacyjnym Schengen, jeżeli stwierdzi, że nie są prawdziwe;

3) wykreślenie jego danych osobowych zawartych w wykazie lub w Systemie Informacyjnym Schengen, jeżeli zostały tam umieszczone w wyniku błędu.",

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

„1a. Wniosek w sprawie danych zawartych w Systemie Informacyjnym Schengen może dotyczyć tylko danych wpisanych przez Szefa Urzędu do Spraw Cudzoziemców do celów odmowy wjazdu.",

c) ust. 3 otrzymuje brzmienie:

„3. W postępowaniu wszczętym wskutek złożenia wniosku, o którym mowa w ust. 1, Szef Urzędu do Spraw Cudzoziemców udziela cudzoziemcowi tylko informacji o wpisaniu jego danych osobowych do wykazu lub do Systemu Informacyjnego Schengen.";

23) w art. 131a dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Przepis ust. 1 stosuje się także do przeglądania dokumentów dotyczących wpisu danych cudzoziemca do Systemu Informacyjnego Schengen dokonanego przez Szefa Urzędu do Spraw Cudzoziemców do celów odmowy wjazdu.";

24) po art. 134 dodaje się art. 134a w brzmieniu:

„Art. 134a. Dane cudzoziemca, z wyłączeniem danych obywateli państw członkowskich Unii Europejskiej, państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stron umowy o Europejskim Obszarze Gospodarczym lub Konfederacji Szwajcarskiej, przechowywane w wykazie na podstawie:

1) art. 128 ust. 1 pkt 1 i 2, z wyłączeniem danych cudzoziemca, który otrzymał decyzję o zobowiązaniu do opuszczenia terytorium Rzeczypospolitej Polskiej,

2) art. 128 ust. 1 pkt 3 i 6,

3) art. 77 ustawy z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin (Dz.U. Nr 144, poz. 1043 oraz z 2007 r. Nr 120, poz. 818)

– są przekazywane do Systemu Informacyjnego Schengen na okres przechowywania ich w wykazie.";

25) w art. 143 w ust. 1:

a) po pkt 4 dodaje się pkt 4a w brzmieniu:

„4a) przekazywanie właściwym organom innych państw obszaru Schengen, za pośrednictwem Komendanta Głównego Policji, informacji dotyczących podstawy prawnej i faktycznej wpisu do celów określonych w art. 25 Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerw-

ca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach;",

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

„5a) wykonywanie funkcji polskiego centralnego organu wizowego;".

Art. 42. W ustawie z dnia 21 lipca 2006 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz.U. Nr 158, poz. 1122) w art. 7 uchyla się ust. 1.

ROZDZIAŁ 8

PRZEPISY PRZEJŚCIOWE I KOŃCOWE

Art. 43. Centralny organ techniczny KSI jest obowiązany do utworzenia oraz uruchomienia Krajowego Systemu Informatycznego w terminie do dnia 1 września 2007 r.

Art. 44. Osoby mające dostęp do Krajowego Systemu Informatycznego po dniu 1 czerwca 2008 r. muszą być przeszkolone w sposób określony w przepisach wydanych na podstawie art. 25 ust. 3, przez osoby posiadające kwalifikacje określone w tych przepisach.

Art. 45. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 52 ust. 1 pkt 1 ustawy, o której mowa w art. 41, zachowują moc do czasu wydania nowych przepisów wykonawczych na podstawie art. 52 ust. 1 pkt 1 ustawy, o której mowa w art. 41, jednakże nie dłużej niż przez okres 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 46. Ustawa wchodzi w życie z dniem ogłoszenia, z tym że:

1) art. 5–7, art. 13 oraz art. 27 ust. 1 pkt 5–7 stosuje się zgodnie z określoną przez Komisję Europejską datą rozpoczęcia funkcjonowania Systemu Informacji Wizowej w Rzeczypospolitej Polskiej;

2) art. 3 ust. 1 pkt 6 i art. 4 ust. 1 pkt 6 wchodzą w życie z dniem określonym w decyzji Rady, zgodnie z art. 55 ust. 2 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SISII) (Dz. Urz. UE L 381 z 28.12.2006, str. 4);

3) art. 41 wchodzi w życie z dniem określonym w decyzji Rady, zgodnie z art. 3 ust. 2 Aktu dotyczącego warunków przystąpienia Republiki Czeskiej, Republiki Estońskiej, Republiki Cypryjskiej, Republiki Łotewskiej, Republiki Litewskiej, Republiki Węgierskiej, Republiki Malty, Rzeczypospolitej Polskiej, Republiki Słowenii i Republiki Słowackiej oraz dostosowań w Traktatach stanowiących podstawę Unii Europejskiej z dnia 16 kwietnia 2003 r. (Dz.U. z 2004 r. Nr 90, poz. 864).

Prezydent Rzeczypospolitej Polskiej: L. Kaczyński

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285 oraz z 2006 r. Nr 104, poz. 708 i 711.

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2005 r. Nr 109, poz. 925, Nr 175, poz. 1462, Nr 179, poz. 1486 i Nr 180, poz. 1494 i 1497, z 2006 r. Nr 17, poz. 141, Nr 104, poz. 708 i 711, Nr 190, poz. 1400, Nr 191, poz. 1410 i Nr 235, poz. 1701 oraz z 2007 r. Nr 52, poz. 343, Nr 57, poz. 381, Nr 99, poz. 661 i Nr 123, poz. 845.

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz.U. z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155, Nr 111, poz. 1061 i Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 626, Nr 93, poz. 889, Nr 240, poz. 2405 i Nr 264, poz. 2641, z 2005 r. Nr 10, poz. 70, Nr 48, poz. 461, Nr 77, poz. 680, Nr 96, poz. 821, Nr 141, poz. 1181, Nr 143, poz. 1203, Nr 163, poz. 1363, Nr 169, poz. 1416 i Nr 178, poz. 1479, z 2006 r. Nr 15, poz. 118, Nr 66, poz. 467, Nr 95, poz. 659, Nr 104, poz. 708 i 711, Nr 141, poz. 1009 i 1013, Nr 167, poz. 1192 i Nr 226, poz. 1647 i 1648 oraz z 2007 r. Nr 20, poz. 116, Nr 64, poz. 432, Nr 80, poz. 539, Nr 89, poz. 589, Nr 99, poz. 664, Nr 112, poz. 766, Nr 123, poz. 849 i Nr 128, poz. 903.

[4)] Zmiany wymienionej ustawy zostały ogłoszone w Dz.U. z 2005 r. Nr 264, poz. 2205, z 2006 r. Nr 170, poz. 1217 i Nr 218, poz. 1592 oraz z 2007 r. Nr 25, poz. 162.

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285 oraz z 2006 r. Nr 104, poz. 708 i 711.