

U S T A W A

z dnia 24 sierpnia 2007 r.

o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym¹⁾

**Opracowano na
podstawie: t.j.
Dz. U. z 2023 r.
poz. 1355, z 2024
r. poz. 1688.**

Rozdział 1

Przepisy ogólne

Art. 1. Ustawa określa zasady i sposób realizacji udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, w tym obowiązki i uprawnienia organów dotyczące dokonywania wpisów oraz wglądu do danych zawartych w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym poprzez Krajowy System Informatyczny (KSI).

Art. 2. Ilekroć w ustawie jest mowa o:

- 1) bezpośrednim dostępie – rozumie się przez to dokonywanie wpisów oraz wgląd do danych przetwarzanych poprzez Krajowy System Informatyczny (KSI), realizowany w sposób bezpośredni przez organ wskazany w ustawie;

¹⁾ Niniejsza ustawa służy stosowaniu:

- 1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz. Urz. UE L 312 z 07.12.2018, str. 1, Dz. Urz. UE L 248 z 13.07.2021, str. 11 oraz Dz. Urz. UE L 249 z 14.07.2021, str. 15);
- 2) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006 (Dz. Urz. UE L 312 z 07.12.2018, str. 14, Dz. Urz. UE L 135 z 22.05.2019, str. 27, Dz. Urz. UE L 248 z 13.07.2021, str. 11 oraz Dz. Urz. UE L 249 z 14.07.2021, str. 15);
- 3) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz. Urz. UE L 312 z 07.12.2018, str. 56, Dz. Urz. UE L 135 z 22.05.2019, str. 85, Dz. Urz. UE L 316 z 06.12.2019, str. 4, Dz. Urz. UE L 248 z 13.07.2021, str. 1, Dz. Urz. UE L 249 z 14.07.2021, str. 1 oraz Dz. Urz. UE L 185 z 12.07.2022, str. 1).

- 2) Centralnym Wizowym Systemie Informacyjnym – rozumie się przez to system centralny, 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. 4 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz. Urz. UE L 312 z 07.12.2018, str. 1, z późn. zm.²⁾), zwanego dalej „rozporządzeniem 2018/1860”, art. 20 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006 (Dz. Urz. UE L 312 z 07.12.2018, str. 14, z późn. zm.³⁾), zwanego dalej „rozporządzeniem 2018/1861”, oraz art. 20 ust. 1–3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz. Urz. UE L 312 z 07.12.2018, str. 56, z późn. zm.⁴⁾), zwanego dalej „rozporządzeniem 2018/1862”;
- 6) danych VIS – rozumie się przez to dane określone w art. 5 ust. 1 rozporządzenia (WE) nr 767/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r.

²⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 248 z 13.07.2021, str. 11 oraz Dz. Urz. UE L 249 z 14.07.2021, str. 15.

³⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 135 z 22.05.2019, str. 27, Dz. Urz. UE L 248 z 13.07.2021, str. 11 oraz Dz. Urz. UE L 249 z 14.07.2021, str. 15.

⁴⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 135 z 22.05.2019, str. 85, Dz. Urz. UE L 316 z 06.12.2019, str. 4, Dz. Urz. UE L 248 z 13.07.2021, str. 1, Dz. Urz. UE L 249 z 14.07.2021, str. 1 oraz Dz. Urz. UE L 185 z 12.07.2022, str. 1.

- w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) (Dz. Urz. UE L 218 z 13.08.2008, str. 60–81);
- 7) informacjach uzupełniających – rozumie się przez to informacje uzupełniające, o których mowa w art. 3 pkt 2 rozporządzenia 2018/1861 oraz art. 3 pkt 2 rozporządzenia 2018/1862;
 - 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) (uchylony)
 - 10) kopii krajowej – rozumie się przez to kopię bazy danych SIS, o której mowa w art. 4 ust. 1 lit. b rozporządzenia 2018/1861 oraz art. 4 ust. 1 lit. b rozporządzenia 2018/1862;
 - 11) Krajowym Systemie Informatycznym (KSI) – rozumie się przez to zespół współpracujących ze sobą urządzeń, procedur przetwarzania informacji i narzędzi programowych (oprogramowania) zastosowanych w celu przetwarzania danych oraz infrastrukturę telekomunikacyjną, umożliwiające organom administracji publicznej i organom wymiaru sprawiedliwości przetwarzanie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym;
 - 12) (uchylony)
 - 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 dokonywanie wpisów oraz wgląd do danych przetwarzanych poprzez Krajowy System Informatyczny (KSI), realizowany w sytuacjach wskazanych w ustawie za pośrednictwem centralnego organu technicznego KSI albo organu wskazanego w art. 7 ust. 2;

- 14a) systemie centralnym SIS – rozumie się przez to system centralny, o którym mowa w art. 4 ust. 1 lit. a rozporządzenia 2018/1861 oraz art. 4 ust. 1 lit. a rozporządzenia 2018/1862;
- 15) Systemie Informacyjnym Schengen – rozumie się przez to system informacyjny, o którym mowa w art. 4 rozporządzenia 2018/1861 oraz art. 4 rozporządzenia 2018/1862;
- 15a) systemie krajowym N.SIS – rozumie się przez to polski system krajowy zawierający kopię krajową, który łączy się z systemem centralnym SIS, spełniający wymagania, o których mowa w art. 4 ust. 1 lit. b rozporządzenia 2018/1861 oraz art. 4 ust. 1 lit. b rozporządzenia 2018/1862;
- 16) Wizowym Systemie Informacyjnym – 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 (VIS);
- 17) wpisie – rozumie się przez to czynności faktyczne polegające na wprowadzeniu do Systemu Informacyjnego Schengen lub Wizowego Systemu Informacyjnego, zmianie lub usunięciu z Systemu Informacyjnego Schengen lub Wizowego Systemu Informacyjnego danych umożliwiających właściwym organom identyfikację osoby lub przedmiotu oraz podjęcie wnioskowanego działania w związku ze zidentyfikowaniem osoby lub przedmiotu;
- 18) przetwarzaniu danych – rozumie się przez to przetwarzanie danych osobowych, o którym mowa w art. 3 pkt 6 rozporządzenia 2018/1861 oraz art. 3 pkt 5 rozporządzenia 2018/1862, a także jakiegokolwiek operacje wykonywane na danych niebędących danymi osobowymi, takie jak zbieranie, wpisywanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
- 19) rozporządzeniu 2016/679 – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.⁵⁾);

⁵⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.
2024-11-29

- 20) tożsamości przywłaszczonej – rozumie się przez to dane wprowadzone do Systemu Informacyjnego Schengen zgodnie z art. 47 rozporządzenia 2018/1861 oraz art. 62 rozporządzenia 2018/1862 dotyczące osoby pokrzywdzonej, której tożsamością posługuje się osoba poszukiwana na podstawie wpisu do Systemu Informacyjnego Schengen;
- 21) odsyłaczu – rozumie się przez to odsyłacz, o którym mowa w art. 48 rozporządzenia 2018/1861 oraz art. 63 rozporządzenia 2018/1862, utworzony w Systemie Informacyjnym Schengen pomiędzy co najmniej dwoma wpisami;
- 22) danych biometrycznych – rozumie się przez to dane, o których mowa w art. 3 pkt 13 rozporządzenia 2018/1861 oraz art. 3 pkt 12 rozporządzenia 2018/1862;
- 23) danych daktyloskopijnych – rozumie się przez to dane, o których mowa w art. 3 pkt 14 rozporządzenia 2018/1861 oraz art. 3 pkt 13 rozporządzenia 2018/1862;
- 24) użytkownika indywidualnym – rozumie się przez to osobę fizyczną upoważnioną w ramach organu do dostępu do Krajowego Systemu Informatycznego (KSI) oraz do przetwarzania danych poprzez Krajowy System Informatyczny (KSI), która w celu dostępu do danych SIS korzysta bezpośrednio z aplikacji WWW SIS, a w celu dostępu do danych VIS korzysta bezpośrednio z aplikacji WWW VIS;
- 25) użytkownika instytucjonalnym – rozumie się przez to organ uprawniony do dostępu i współpracy z Krajowym Systemem Informatycznym (KSI) za pośrednictwem własnego systemu teleinformatycznego;
- 26) użytkownika końcowym – rozumie się przez to osobę fizyczną upoważnioną do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI) za pośrednictwem systemu teleinformatycznego użytkownika instytucjonalnego;
- 27) aplikacji WWW SIS – rozumie się przez to graficzny interfejs użytkownika Krajowego Systemu Informatycznego (KSI), stanowiący informatyczne narzędzie dostępowe do danych SIS udostępnione użytkownikowi indywidualnemu przez centralny organ techniczny KSI;
- 28) aplikacji WWW VIS – rozumie się przez to graficzny interfejs użytkownika Krajowego Systemu Informatycznego (KSI), stanowiący informatyczne

narzędzie dostępne do danych VIS udostępnione użytkownikowi indywidualnemu przez centralny organ techniczny KSI;

- <29)⁶⁾ danych EES – rozumie się przez to dane, o których mowa w art. 3 ust. 1 pkt 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiającego system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określającego warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniającego konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz. Urz. UE L 327 z 09.12.2017, str. 20, z późn. zm.⁷⁾), zwanego dalej „rozporządzeniem 2017/2226”;
- 30)⁶⁾ systemie EES – rozumie się przez to System Wjazdu/Wyjazdu (EES), o którym mowa w art. 7 rozporządzenia 2017/2226.>

Rozdział 2

Organy i służby uprawnione do przetwarzania danych

Art. 3. 1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS dotyczących:

- 1) osób poszukiwanych do tymczasowego aresztowania w celu wydania ich przez państwo obce na podstawie wniosku o wydanie – przysługuje sądowi lub prokuraturze;
- 2) osób poszukiwanych do tymczasowego aresztowania w celu przekazania osoby ściganej na podstawie europejskiego nakazu aresztowania lub na podstawie nakazu aresztowania wydanego zgodnie z zawartą w tym celu umową, która

⁶⁾ Dodane pkt 29 i 30 w art. 2 wejdą w życie z dniem określonym w decyzji Komisji Europejskiej, zgodnie z art. 66 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiającego system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określającego warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniającego konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011.

⁷⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 236 z 19.01.2018, str. 1, Dz. Urz. UE L 258 z 15.10.2018, str. 5, Dz. Urz. UE L 117 z 03.05.2019, str. 13, Dz. Urz. UE L 135 z 22.05.2019, str. 27, Dz. Urz. UE L 248 z 13.07.2021, str. 11, Dz. Urz. UE L 249 z 14.07.2021, str. 15 oraz Dz. Urz. UE L 2024/1356 z 22.05.2024.

- przewiduje przekazywanie takiego nakazu aresztowania za pośrednictwem Systemu Informacyjnego Schengen – przysługuje sądowi lub prokuraturze;
- 3) świadków albo podejrzanych lub oskarżonych wezwanych do stawiennictwa przed sądem lub prokuratorem celem złożenia wyjaśnień w związku z postępowaniem karnym lub postępowaniem karnym skarbowym lub poszukiwanych w celu wezwania do takiego stawiennictwa albo osób, którym ma zostać doręczony wyrok w sprawie karnej lub w sprawie o przestępstwo skarbowe lub inne dokumenty związane z postępowaniem karnym lub postępowaniem karnym skarbowym w celu złożenia wyjaśnień, albo osób, którym ma zostać doręczone wezwanie do stawienia się w celu odbycia kary pozbawienia wolności – w celu zapewnienia informacji o ich miejscu zamieszkania lub pobytu – przysługuje sądowi lub prokuraturze;
 - 4) cudzoziemców objętych odmową wjazdu i pobytu na warunkach określonych w art. 24 rozporządzenia 2018/1861 – przysługuje Szefowi Urzędu do Spraw Cudzoziemców;
 - 5) cudzoziemców, w stosunku do których została wydana decyzja o zobowiązaniu cudzoziemca do powrotu na zasadach określonych w art. 3 rozporządzenia 2018/1860 – przysługuje Straży Granicznej;
 - 6) osób zaginionych, które dla ich własnej ochrony lub w celu zapobieżenia stwarzanemu przez nie zagrożeniu dla porządku publicznego lub bezpieczeństwa publicznego powinny zostać umieszczone we właściwej placówce opiekuńczej lub leczniczej, w szczególności w wyniku decyzji o przymusowym umieszczeniu w takiej placówce, oraz osób zaginionych, które nie wymagają ochrony – przysługuje Policji;
 - 7) małoletnich, którym należy uniemożliwić podróżowanie ze względu na zagrożenie uprowadzeniem przez rodzica, członka rodziny lub opiekuna lub ze względu na realne zagrożenie, że zostaną wywiezieni z terytorium państwa członkowskiego lub opuszczą to terytorium – przysługuje Policji, sądowi lub prokuraturze;
 - 8) małoletnich, którym należy uniemożliwić podróżowanie ze względu na realne zagrożenie, że zostaną wywiezieni z terytorium państwa członkowskiego lub opuszczą to terytorium oraz że staną się ofiarami handlu ludźmi lub ofiarami przymusowego małżeństwa, okaleczenia żeńskich narządów płciowych lub

innych form przemocy warunkowanej płcią – przysługuje Policji, Straży Granicznej, sądowi lub prokuraturze;

- 9) małoletnich, którym należy uniemożliwić podróżowanie ze względu na realne zagrożenie, że zostaną wywiezieni z terytorium państwa członkowskiego lub opuszczą to terytorium oraz że staną się ofiarami przestępstw o charakterze terrorystycznym lub wezmą udział w popełnianiu takich przestępstw lub zostaną zwerbowani lub zaciągnięci do ugrupowań zbrojnych, lub zmuszeni do aktywnego udziału w działaniach wojennych – przysługuje Policji, Agencji Bezpieczeństwa Wewnętrznego, sądowi lub prokuraturze;
- 10) osób pełnoletnich narażonych na niebezpieczeństwo, którym dla ich własnej ochrony należy uniemożliwić podróżowanie ze względu na realne zagrożenie, że zostaną wywiezione z terytorium państwa członkowskiego lub opuszczą to terytorium oraz że staną się ofiarami handlu ludźmi lub przemocy warunkowanej płcią – przysługuje Policji, Straży Granicznej, sądowi lub prokuraturze;
- 11) osób lub przedmiotów należących do jednej z kategorii, o których mowa w pkt 12 lit. a–c, e, g, h oraz j–l, a także bezgotówkowych środków płatniczych wprowadzonych w celu:
 - a) przeprowadzania kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych, których celem jest zapobieganie przestępstwom, ich wykrywanie, prowadzenie w ich sprawie postępowań przygotowawczych lub ich ściganie, wykonanie wyroku w sprawach karnych lub w sprawach o przestępstwa skarbowe lub zapobieganie zagrożeniom dla bezpieczeństwa publicznego, jeżeli zachodzi co najmniej jedna z następujących okoliczności:
 - istnieje uzasadnione podejrzenie, że dana osoba ma zamiar popełnić lub popełnia którekolwiek z przestępstw, o których mowa w art. 607w ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2022 r. poz. 1375, z późn. zm.⁸⁾),
 - informacje, o których mowa w art. 37 ust. 1 rozporządzenia 2018/1862, są niezbędne do wykonania kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w odniesieniu do osoby skazanej za popełnienie któregośkolwiek

⁸⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1855, 2582 i 2600 oraz z 2023 r. poz. 289, 535 i 818.

- z przestępstw, o których mowa w art. 607w ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego,
- ogólna ocena danej osoby, w szczególności w świetle wcześniej popełnionych przestępstw, pozwala przypuszczać, że osoba ta może w przyszłości popełnić przestępstwo, o którym mowa w art. 607w ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego
 - przysługuje Policji, Służbie Celno-Skarbowej, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej lub Centralnemu Biuru Antykorupcyjnemu,
- b) przeprowadzania kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych, których celem jest zapobieganie poważnym zagrożeniom wewnętrznego i zewnętrznego bezpieczeństwa państwa – przysługuje Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Ochrony Państwa, Służbie Kontrwywiadu Wojskowego lub Służbie Wywiadu Wojskowego;
- 12) przedmiotów podlegających zatrzymaniu albo mogących stanowić dowód w sprawie lub podlegających zajęciu w celu zabezpieczenia w postępowaniu karnym lub postępowaniu karnym skarbowym, należących do jednej z poniższych kategorii:
- a) pojazdy silnikowe niezależnie od układu napędowego,
 - b) przyczepy o masie własnej przekraczającej 750 kg,
 - c) przyczepy turystyczne,
 - d) urządzenia przemysłowe,
 - e) jednostki pływające,
 - f) silniki jednostek pływających,
 - g) kontenery,
 - h) statki powietrzne,
 - i) silniki statków powietrznych,
 - j) broń palna,
 - k) blankiety dokumentów urzędowych, które zostały skradzione, przywłaszczone, utracone lub które mają charakter takich dokumentów, ale są fałszywe,
 - l) wydane dokumenty tożsamości, takie jak paszporty, dowody tożsamości, dokumenty pobytowe, dokumenty podróży oraz prawa jazdy, które zostały

skradzione, przywłaszczone, utracone lub unieważnione lub które mają charakter takich dokumentów, ale są fałszywe,

- m) dowody rejestracyjne pojazdów i tablice rejestracyjne pojazdów, które zostały skradzione, przywłaszczone, utracone lub unieważnione lub które mają charakter takich dokumentów lub tablic rejestracyjnych, ale są fałszywe,
- n) banknoty o spisanych numerach i banknoty fałszywe,
- o) sprzęt informatyczny,
- p) możliwe do zidentyfikowania części pojazdów silnikowych,
- q) możliwe do zidentyfikowania części urządzeń przemysłowych,
- r) inne możliwe do zidentyfikowania przedmioty o znacznej wartości, zdefiniowane zgodnie z art. 38 ust. 3 rozporządzenia 2018/1862

– przysługuje Policji, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

- 13) przedmiotów podlegających zatrzymaniu, należących do jednej z kategorii:
 - a) blankiety dokumentów urzędowych, które zostały skradzione, przywłaszczone lub utracone,
 - b) wydane dokumenty tożsamości, takie jak paszporty, dowody tożsamości, dokumenty pobytowe, dokumenty podróży oraz prawa jazdy, które zostały skradzione, przywłaszczone, utracone lub unieważnione– przysługuje ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw zagranicznych, Szefowi Urzędu do Spraw Cudzoziemców lub wojewodzie;
- 14) podlegających zatrzymaniu dowodów rejestracyjnych pojazdów i tablic rejestracyjnych pojazdów, które zostały skradzione, przywłaszczone, utracone lub unieważnione – przysługuje ministrowi właściwemu do spraw wewnętrznych;
- 15) danych daktyloskopijnych znalezionych na miejscu popełnienia przestępstw o charakterze terrorystycznym lub innych poważnych przestępstw będących przedmiotem postępowania przygotowawczego, jeżeli zachodzi bardzo wysokie prawdopodobieństwo, że należą do sprawcy – przysługuje Agencji Bezpieczeństwa Wewnętrznego, Centralnemu Biuru Antykorupcyjnemu, Policji, Służbie Celno-Skarbowej, Żandarmerii Wojskowej lub Straży Granicznej.

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

3. Organy wymienione w ust. 1 odpowiadają za wprowadzone wpisy danych SIS, w tym dokonują ich aktualizacji, weryfikacji, przedłużenia okresu utrzymywania i usunięcia na zasadach określonych w art. 39 ust. 1–5 i 7, art. 40 i art. 44 rozporządzenia 2018/1861 oraz art. 53 ust. 1–7 i 9, art. 54 ust. 1–4, art. 55 i art. 59 rozporządzenia 2018/1862.

4. W przypadku operacji, o której mowa w art. 26 ust. 4 rozporządzenia 2018/1862, o zgodę na tymczasowy brak dostępności do wglądu danych SIS zawartych w istniejącym wpisie, o którym mowa w ust. 1 pkt 1 i 2, do sądu lub prokuratury albo organu wymiaru sprawiedliwości innego państwa, który wprowadził wpis, może wystąpić Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego lub Centralne Biuro Antykorupcyjne.

5. W przypadku gdy decyzja, o której mowa w ust. 1 pkt 5, została zrealizowana zgodnie z art. 6 rozporządzenia 2018/1860 i towarzyszy jej zakaz wjazdu, o którym mowa w art. 24 ust. 1 lit. b rozporządzenia 2018/1861, Szefowi Urzędu do Spraw Cudzoziemców przysługuje możliwość dokonania wpisu określonego w ust. 1 pkt 4 w miejsce wpisu określonego w ust. 1 pkt 5 zgodnie z art. 24 rozporządzenia 2018/1861.

6. W celu dokonania wpisu do Systemu Informacyjnego Schengen określonego w ust. 1 pkt 5, pozwalającego na skuteczną identyfikację osoby nim objętej, organ uprawniony przetwarza dane SIS zgodnie z zakresem wskazanym w art. 4 rozporządzenia 2018/1860. W celu dokonania wpisu do Systemu Informacyjnego Schengen określonego w ust. 1 pkt 1–4 i 6–15, pozwalającego na skuteczną identyfikację osoby nim objętej, organy uprawnione przetwarzają dane SIS zgodnie z zakresem wskazanym w art. 20 rozporządzenia 2018/1861 oraz art. 20 rozporządzenia 2018/1862.

Art. 3a. (uchylony)

Art. 3b. Dostęp do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS, o których mowa w art. 3 ust. 1 pkt 1–3, 7–10 i 12,

sądy realizują za pośrednictwem systemu teleinformatycznego prowadzonego przez Ministra Sprawiedliwości.

Art. 4. 1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych SIS dotyczących:

- 1) osób poszukiwanych do tymczasowego aresztowania w celu wydania ich na wniosek państwa członkowskiego lub państwa obcego – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, Służbie Ochrony Państwa, ministrowi właściwemu do spraw wewnętrznych, wojewodzie, sądowi lub prokuraturze;
- 2) osób poszukiwanych do tymczasowego aresztowania, o których mowa w art. 3 ust. 1 pkt 2 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, Służbie Ochrony Państwa, ministrowi właściwemu do spraw wewnętrznych, wojewodzie, sądowi lub prokuraturze;
- 3) osób poszukiwanych w celu zapewnienia informacji o ich miejscu zamieszkania lub pobytu, o których mowa w art. 3 ust. 1 pkt 3 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, Służbie Ochrony Państwa, sądowi lub prokuraturze;
- 4) cudzoziemców, o których mowa w art. 3 ust. 1 pkt 4 – przysługuje ministrowi właściwemu do spraw zagranicznych, ministrowi właściwemu do spraw wewnętrznych, Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Służbie Celno-Skarbowej, Służbie Ochrony Państwa, Szefowi Urzędu do Spraw Cudzoziemców, wojewodzie, konsulowi, sądowi lub prokuraturze;
- 5) cudzoziemców, o których mowa w art. 3 ust. 1 pkt 5 – przysługuje ministrowi właściwemu do spraw zagranicznych, ministrowi właściwemu do spraw wewnętrznych, Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu

Wojskowego, Służbie Celno-Skarbowej, Służbie Ochrony Państwa, Szefowi Urzędu do Spraw Cudzoziemców, wojewodzie, konsulowi, sądowi lub prokuraturze;

- 6) osób zaginionych, o których mowa w art. 3 ust. 1 pkt 6 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, Służbie Ochrony Państwa, ministrowi właściwemu do spraw wewnętrznych, wojewodzie, sądowi lub prokuraturze;
- 7) małoletnich, o których mowa w art. 3 ust. 1 pkt 7 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;
- 8) małoletnich, o których mowa w art. 3 ust. 1 pkt 8 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;
- 9) małoletnich, o których mowa w art. 3 ust. 1 pkt 9 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;
- 10) osób pełnoletnich narażonych na niebezpieczeństwo, o których mowa w art. 3 ust. 1 pkt 10 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;
- 11) osób lub przedmiotów wprowadzonych w celu przeprowadzania kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych, o których mowa w art. 3 ust. 1 pkt 11 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Żandarmerii Wojskowej, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, Służbie Ochrony Państwa, ministrowi właściwemu do spraw wewnętrznych, wojewodzie, sądowi lub prokuraturze;
- 12) przedmiotów, o których mowa w art. 3 ust. 1 pkt 12 – przysługuje Straży Granicznej, Policji, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii

Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Służbie Celno-Skarbowej, sądowi lub prokuraturze;

- 13) przedmiotów podlegających zatrzymaniu albo mogących stanowić dowód w sprawie lub podlegających zajęciu w celu zabezpieczenia w postępowaniu karnym lub postępowaniu karnym skarbowym, należących do jednej z kategorii, o których mowa w art. 3 ust. 1 pkt 12 lit. k oraz l – przysługuje ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw zagranicznych, Szefowi Urzędu do Spraw Cudzoziemców, wojewodzie lub konsulowi;
- 14) przedmiotów podlegających zatrzymaniu albo mogących stanowić dowód w sprawie lub podlegających zajęciu w celu zabezpieczenia w postępowaniu karnym lub postępowaniu karnym skarbowym, należących do jednej z kategorii, o których mowa w art. 3 ust. 1 pkt 12 lit. a–i, m, p oraz q – przysługuje ministrowi właściwemu do spraw wewnętrznych, Służbie Ochrony Państwa, Agencji Wywiadu, Służbie Wywiadu Wojskowego, Służbie Kontrwywiadu Wojskowego lub wojewodzie mazowieckiemu;
- 15) przedmiotów podlegających zatrzymaniu albo mogących stanowić dowód w sprawie lub podlegających zajęciu w celu zabezpieczenia w postępowaniu karnym lub postępowaniu karnym skarbowym, należących do jednej z kategorii, o których mowa w art. 3 ust. 1 pkt 12 lit. a, e oraz h – przysługuje naczelnikowi urzędu skarbowego;
- 16) przedmiotów, o których mowa w art. 3 ust. 1 pkt 12 lit. h oraz i – przysługuje Prezesowi Urzędu Lotnictwa Cywilnego;
- 17) danych daktyloskopijnych, o których mowa w art. 3 ust. 1 pkt 15, jeżeli zachodzi wysokie prawdopodobieństwo, że należą do sprawcy – przysługuje Agencji Bezpieczeństwa Wewnętrznego, Policji, Żandarmerii Wojskowej, Służbie Celno-Skarbowej, Centralnemu Biuru Antykorupcyjnemu lub Straży Granicznej.

2. Uprawnienie do pośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych SIS dotyczących przedmiotów, o których mowa w art. 3 ust. 1 pkt 12 lit. a–c, m oraz p – przysługuje organom jednostek samorządu terytorialnego właściwym w sprawach rejestracji pojazdów.

3. Uprawnienie do pośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych SIS dotyczących przedmiotów, o których mowa w art. 3 ust. 1 pkt 12 lit. e oraz f – przysługuje dyrektorowi urzędu

morskiego, izbie morskiej, dyrektorowi urzędu żeglugi śródlądowej oraz organom rejestrującym w rozumieniu art. 2 pkt 8 ustawy z dnia 12 kwietnia 2018 r. o rejestracji jachtów i innych jednostek pływających o długości do 24 m (Dz. U. z 2020 r. poz. 1500, z 2022 r. poz. 2642 oraz z 2023 r. poz. 261).

4. Uprawnienie do wglądu do danych SIS przysługuje organom określonym w:

- 1) ust. 1 pkt 14 i ust. 2 wyłącznie w związku z wykonywaniem obowiązku rejestracji pojazdów określonego w art. 73 i art. 74 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2022 r. poz. 988, z późn. zm.⁹⁾) w celu sprawdzenia, czy zgłoszone do rejestracji pojazdy oraz towarzyszące im dowody rejestracyjne i tablice rejestracyjne nie zostały skradzione, przywłaszczone, utracone lub nie są poszukiwane jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym;
- 2) ust. 1 pkt 16 wyłącznie w związku z wykonywaniem obowiązku rejestracji statków powietrznych określonego w art. 34, art. 35 i art. 37 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2022 r. poz. 1235, 1715, 1846, 2185 i 2642) albo obowiązku ich wpisu do ewidencji określonego w przepisach wydanych na podstawie art. 33 ust. 2 i 4 tej ustawy w celu sprawdzenia, czy statki powietrzne zgłoszone do rejestracji albo ewidencji lub ich silniki nie zostały skradzione, przywłaszczone, utracone lub nie są poszukiwane jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym;
- 3) ust. 3 wyłącznie w związku z wykonywaniem obowiązku rejestracji jednostek pływających określonego w art. 23 i art. 39 ustawy z dnia 18 września 2001 r. – Kodeks morski (Dz. U. z 2018 r. poz. 2175, z 2022 r. poz. 2642 oraz z 2023 r. poz. 261), art. 18 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2022 r. poz. 1097 i 2642) oraz art. 4 ustawy z dnia 12 kwietnia 2018 r. o rejestracji jachtów i innych jednostek pływających o długości do 24 m w celu sprawdzenia, czy zgłoszone do rejestracji jednostki pływające, w tym silniki jednostek pływających, nie zostały skradzione, przywłaszczone, utracone lub nie są poszukiwane jako dowód w postępowaniu karnym lub postępowaniu karnym skarbowym.

5. Organy, o których mowa w ust. 1, w przypadku odnalezienia na skutek wglądu do danych SIS osoby lub przedmiotu, których dotyczy wpis, są obowiązane

⁹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1002, 1768, 1783, 2589, 2600 i 2642 oraz z 2023 r. poz. 760 i 919.

bezzwłocznie poinformować o tym odpowiednio organ wymieniony w art. 3, który dokonał wpisu, albo biuro SIRENE oraz podjąć wnioskowane we wpisie działania, o ile realizowane przez dany organ zadania umożliwiają mu takie działania, albo bezzwłocznie przekazać osobę lub przedmiot Policji. Przy realizacji tych obowiązków organy korzystają w szczególności z formularzy odnalezienia osoby, odnalezienia przedmiotu, tożsamości przywłaszczonej, oświadczenia o wyrażeniu zgody na uzupełnienie danych SIS oraz protokołu przekazania osoby.

6. Organy, o których mowa w ust. 2 i 3, w przypadku odnalezienia na skutek wglądu do danych SIS przedmiotu, którego dotyczy wpis, są obowiązane podjąć wnioskowane we wpisie działania, bezzwłocznie informując odpowiednio organ wymieniony w art. 3, który dokonał wpisu, albo biuro SIRENE, albo bezzwłocznie przekazać przedmiot Policji, a w razie braku takiej możliwości bezzwłocznie przekazać Policji informację o odnalezieniu przedmiotu.

7. W przypadku przekazania osoby lub przedmiotu albo informacji, o której mowa w ust. 6, Policja podejmuje wnioskowane we wpisie działania na podstawie ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2023 r. poz. 171, z późn. zm.¹⁰⁾), bezzwłocznie informując odpowiednio organ wymieniony w art. 3, który dokonał wpisu, albo biuro SIRENE oraz stosuje inne przewidziane prawem środki w oparciu o przekazane wraz z osobą lub przedmiotem materiały, w szczególności treść zgromadzonej w związku z zatrzymaniem dokumentacji.

8. Dokumenty, o których mowa w ust. 5, zawierają:

- 1) formularz odnalezienia osoby:
 - a) nazwisko,
 - b) imiona,
 - c) nazwisko rodowe,
 - d) wcześniej używane nazwiska,
 - e) datę, miejsce i kraj urodzenia,
 - f) obywatelstwo,
 - g) płeć,
 - h) informacje o innej tożsamości,
 - i) dane posiadanego dokumentu tożsamości:
 - rodzaj dokumentu,

¹⁰⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 2600 oraz z 2023 r. poz. 185, 240, 289, 347, 535 i 641.

- seria i numer dokumentu,
 - kraj wydania,
 - data wydania i ważności,
- j) dane dotyczące zezwolenia na pobyt lub wizy długoterminowej:
- rodzaj i numer dokumentu,
 - kraj wydania,
 - okres ważności,
- k) dane osób towarzyszących osobie odnalezionej:
- imiona i nazwisko,
 - data urodzenia,
- l) inne dane określone w aktach wykonawczych przyjętych przez Komisję Europejską na podstawie art. 8 ust. 4, art. 9 ust. 5, art. 20 ust. 3 i art. 32 ust. 4 rozporządzenia 2018/1861 oraz art. 8 ust. 4, art. 9 ust. 5, art. 12 ust. 8, art. 20 ust. 4, art. 26 ust. 6, art. 32 ust. 9, art. 34 ust. 3, art. 36 ust. 6, art. 38 ust. 4, art. 42 ust. 5 i art. 62 ust. 4 rozporządzenia 2018/1862, służące realizacji procedury wymiany informacji uzupełniających;
- 2) formularz odnalezienia przedmiotu:
- a) dane osoby posiadającej lub osób posiadających odnaleziony przedmiot:
- imiona,
 - nazwisko,
 - data urodzenia,
 - opis osoby posiadającej lub osób posiadających odnaleziony przedmiot,
- b) dane osób towarzyszących osobie posiadającej odnaleziony przedmiot:
- imiona i nazwisko,
 - data urodzenia,
- c) dane osoby upoważnionej, która sporządziła i nadała formularz:
- imię i nazwisko,
 - jednostka organizacyjna i organ,
 - telefon służbowy lub faks i adres poczty elektronicznej,
 - podpis lub odpowiednio dla wersji elektronicznej numer identyfikacyjny w systemie,
- d) dane dotyczące osoby powiązanej z zabezpieczonym przedmiotem:
- nazwisko,

- imiona,
 - nazwisko rodowe,
 - data urodzenia,
 - miejsce urodzenia,
 - płeć,
 - obywatelstwo,
 - inne posiadane tożsamości,
 - dane dotyczące posiadanego dokumentu tożsamości (seria, numer, data wydania, kraj wydania dokumentu tożsamości),
- e) dane dotyczące dokumentu (blankietu dokumentu, wydanego dokumentu tożsamości, dokumentu pobytowego, dokumentu podróży, prawa jazdy oraz dowodu rejestracyjnego pojazdu):
- nazwisko,
 - imiona,
 - nazwisko rodowe,
 - data urodzenia,
 - miejsce urodzenia,
 - płeć,
 - obywatelstwo,
 - inne posiadane tożsamości,
- f) dane dotyczące prawowitego właściciela:
- nazwisko,
 - imiona,
 - nazwisko rodowe,
 - data urodzenia,
 - miejsce urodzenia,
 - płeć,
 - obywatelstwo,
 - inne posiadane tożsamości,
 - posiadany dokument tożsamości (seria, numer, nazwa organu, który wydał dokument oraz data jego wydania),
- g) inne dane określone w aktach wykonawczych przyjętych przez Komisję Europejską na podstawie art. 8 ust. 4, art. 9 ust. 5, art. 20 ust. 3 i art. 32 ust. 4 rozporządzenia 2018/1861 oraz art. 8 ust. 4, art. 9 ust. 5,

art. 12 ust. 8, art. 20 ust. 4, art. 26 ust. 6, art. 32 ust. 9, art. 34 ust. 3, art. 36 ust. 6, art. 38 ust. 4, art. 42 ust. 5 i art. 62 ust. 4 rozporządzenia 2018/1862, służące realizacji procedury wymiany informacji uzupełniających;

3) formularz tożsamości przywłaszczonej:

a) dane tożsamości przywłaszczonej:

- nazwisko,
- imiona,
- nazwisko rodowe,
- wcześniej używane nazwiska,
- data, miejsce i kraj urodzenia,
- obywatelstwa,
- płeć,

b) informacje o innej tożsamości:

- nazwisko,
- imiona,
- nazwisko rodowe,
- wcześniej używane nazwiska,
- data, miejsce i kraj urodzenia,
- obywatelstwa,
- płeć,

c) dane dotyczące dokumentu:

- rodzaj dokumentu,
- kraj wydania,
- numer dokumentu,
- data i miejsce wydania,
- organ wydający,
- data ważności,
- imię i nazwisko ojca oraz imię i nazwisko matki,

d) aktualny adres zamieszkania:

- kraj zamieszkania lub pobytu,
- województwo lub region,
- miejscowość zamieszkania,
- ulica, kod pocztowy,

- miejscowość poczty,
 - numer telefonu lub inne dane kontaktowe,
 - inne dane dotyczące miejsca zamieszkania,
- e) inne dane określone w aktach wykonawczych przyjętych przez Komisję Europejską na podstawie art. 8 ust. 4, art. 9 ust. 5, art. 20 ust. 3 i art. 32 ust. 4 rozporządzenia 2018/1861 oraz art. 8 ust. 4, art. 9 ust. 5, art. 12 ust. 8, art. 20 ust. 4, art. 26 ust. 6, art. 32 ust. 9, art. 34 ust. 3, art. 36 ust. 6, art. 38 ust. 4, art. 42 ust. 5 i art. 62 ust. 4 rozporządzenia 2018/1862, służące realizacji procedury wymiany informacji uzupełniających;
- 4) oświadczenie o wyrażeniu zgody na uzupełnienie danych SIS:
- a) zgodę na uzupełnienie danych SIS w celu rozwiązywania problemów związanych z przywłaszczaniem tożsamości o imiona i nazwisko, nazwisko rodowe, miejsce i datę urodzenia, płeć danej osoby oraz jej fotografie, odbitki linii papilarnych, posiadany przez nią dokument lub dokumenty tożsamości wraz z danymi identyfikacyjnymi każdego z tych dokumentów, a także o poprzednio używane imiona i nazwiska, inne posiadane tożsamości, szczególne obiektywne cechy fizyczne niepodlegające zmianom, posiadane obywatelstwa, adres zamieszkania danej osoby oraz imiona i nazwiska jej rodziców,
 - b) potwierdzenie okoliczności przekazania informacji o celu dostępności i wykorzystania objętych zgodą danych,
 - c) potwierdzenie świadomości osoby udzielającej zgody co do istnienia możliwości cofnięcia zgody w każdym czasie,
 - d) datę i podpis osoby udzielającej zgody;
- 5) protokół przekazania osoby:
- a) nazwę i numer rejestru albo znak sprawy,
 - b) nazwę jednostki organizacyjnej przekazującej osobę i miejsce przekazania,
 - c) datę, godzinę i miejsce sporządzenia protokołu oraz datę i godzinę przekazania protokołu,
 - d) stopień, imię i nazwisko osoby przekazującej i osoby przejmującej, a także ich stanowiska, nazwy jednostek i komórek organizacyjnych oraz inne informacje niezbędne do określenia przynależności służbowej tych osób,

- e) nazwisko, imiona, nazwisko rodowe, datę i miejsce urodzenia, numer tożsamości, płeć, obywatelstwo, rysopis osoby przekazywanej oraz jej numer ID Schengen, a także posiadany przez nią dokument tożsamości wraz z danymi identyfikacyjnymi tego dokumentu,
- f) nazwiska, imiona, stopień, stanowiska lub pełnione funkcje innych osób uczestniczących w przekazaniu oraz nazwy jednostek i komórek organizacyjnych lub reprezentowanego przez nie podmiotu oraz inne informacje niezbędne do określenia przynależności służbowej tych osób,
- g) uwagi dotyczące przekazania oraz uwagi dotyczące skreśleń i poprawek,
- h) wykaz rzeczy oraz dokumentów przekazanych wraz z osobą,
- i) podpisy osób biorących udział w czynności.

9. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb przekazywania Policji osób lub przedmiotów odnalezionych na skutek wglądu do danych SIS, procedurę postępowania w przypadkach ujawnienia tożsamości przywłaszczonej oraz sposób i tryb współpracy organów z biurem SIRENE, w tym procedurę wymiany informacji uzupełniających określonych w art. 37 ust. 2 niezbędnych do wykonania wnioskowanych we wpisie działań, a także wzory dokumentów, o których mowa w ust. 5, uwzględniając sprawną i skuteczną realizację wnioskowanych we wpisie działań wobec odnalezionych osób lub przedmiotów.

10. Uprawnienie do weryfikacji dopasowań uzyskanych przez uprawniony organ, opierających się na porównaniu danych biometrycznych, przysługuje Centralnemu Laboratorium Kryminalistycznemu Policji.

11. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób i tryb przetwarzania danych biometrycznych oraz sposób i tryb weryfikacji dopasowań opartych na porównaniu danych daktyloskopijnych, uwzględniając procedurę postępowania i warunki techniczne przy pobieraniu, rejestrowaniu i przekazywaniu tych danych.

Art. 4a. (uchylony)

Art. 4b. Dostęp do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych SIS, o których mowa w art. 4 ust. 1 pkt 1–12, sądy realizują za pośrednictwem systemu teleinformatycznego prowadzonego przez Ministra Sprawiedliwości.

Art. 5. 1. Bezpośredni dostęp do Wizowego Systemu Informacyjnego jest realizowany poprzez Krajowy System Informatyczny (KSI) w celu dokonywania wpisów danych VIS przez Straż Graniczną, konsula, wojewodę, ministra właściwego do spraw zagranicznych lub Szefa Urzędu do Spraw Cudzoziemców.

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

- 1) wymiany krajowych danych VIS przez dokonywanie wpisów do Centralnego Wizowego Systemu Informacyjnego poprzez Krajowy System Informatyczny (KSI);
- 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 danych VIS po upływie okresu, na który dane te zostały przez dany organ wprowadzone;
- 4) niezwłocznego informowania centralnego organu technicznego KSI o ujawnionych nieprawidłowościach w związku z wykorzystaniem danych VIS poprzez Krajowy System Informatyczny (KSI);
- 5) rozpatrzenia wniosków państw członkowskich o dokonanie zmiany lub usunięcia danych VIS wprowadzonych przez dany organ oraz powiadomienia państw członkowskich o konieczności dokonania zmiany lub usunięcia danych VIS wprowadzonych przez te państwa członkowskie.

3. Konsul lub wojewoda niezwłocznie powiadamiają państwo członkowskie lub państwa członkowskie o nabyciu obywatelstwa polskiego przez osobę ubiegającą się o wizę w tym państwie członkowskim lub państwach członkowskich.

Art. 6. Bezpośredni dostęp do Wizowego Systemu Informacyjnego realizowany poprzez Krajowy System Informatyczny (KSI) umożliwiający wgląd do danych VIS w celu:

- 1) rozpatrzenia złożonych wniosków wizowych oraz podjęcia decyzji dotyczących tych wniosków, jak również decyzji o unieważnieniu, przedłużeniu, cofnięciu wizy, przysługuje Straży Granicznej, konsulowi, wojewodzie, ministrowi właściwemu do spraw zagranicznych lub Szefowi Urzędu do Spraw Cudzoziemców;
- 2) przeprowadzania konsultacji między centralnymi organami wizowymi w sprawie wniosków wizowych zgodnie z art. 22 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiającego

- Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz. Urz. UE L 243 z 15.09.2009, str. 1) przysługuje Szefowi Urzędu do Spraw Cudzoziemców;
- 3) sporządzania sprawozdań i statystyk, przysługuje Straży Granicznej, konsulowi, wojewodzie, ministrowi właściwemu do spraw zagranicznych lub Szefowi Urzędu do Spraw Cudzoziemców;
 - 4) sprawdzenia na przejściach granicznych tożsamości posiadacza wizy, autentyczności wizy lub spełnienia warunków wjazdu na terytorium państw członkowskich zgodnie z art. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz. Urz. UE L 77/1 z 23.03.2016) przysługuje Straży Granicznej i Służbie Celno-Skarbowej;
 - 5) sprawdzania na terytorium Rzeczypospolitej Polskiej tożsamości posiadacza wizy, autentyczności wizy lub spełnienia warunków wjazdu lub pobytu na terytorium państw członkowskich przysługuje komendantowi wojewódzkiemu Policji, komendantowi powiatowemu (miejskiemu) Policji, komendantowi oddziału Straży Granicznej lub komendantowi placówki Straży Granicznej, Służbie Celno-Skarbowej, wojewodzie lub Szefowi Urzędu do Spraw Cudzoziemców;
 - 6) zidentyfikowania osoby, która nie spełnia lub przestała spełniać warunki wjazdu lub pobytu na terytorium państw członkowskich, przysługuje Straży Granicznej, Policji, Służbie Celno-Skarbowej, wojewodzie lub Szefowi Urzędu do Spraw Cudzoziemców;
 - 7) określania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej zgodnie z art. 12 i art. 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (wersja przekształcona) (Dz. Urz. UE L 180 z 29.06.2013) przysługuje Szefowi Urzędu do Spraw Cudzoziemców;
 - 8) rozpatrzenia wniosku o udzielenie ochrony międzynarodowej przysługuje Szefowi Urzędu do Spraw Cudzoziemców lub Radzie do Spraw Uchodźców;

- 9) realizacji obowiązku, o którym mowa w art. 25 ust. 2 rozporządzenia (WE) nr 767/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), przysługuje konsulowi lub wojewodzie.

<Art. 6a.¹¹⁾ W związku z ustanowieniem interoperacyjności między systemem EES i Wizowym Systemem Informacyjnym, o której mowa w art. 8 rozporządzenia 2017/2226 oraz w art. 17a rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany informacji pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, wiz długoterminowych i dokumentów pobytowych (rozporządzenie w sprawie VIS):

- 1) organy, o których mowa w art. 5 ust. 1, mogą dokonać wglądu do danych EES z poziomu VIS w celach, o których mowa w art. 17a ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany informacji pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, wiz długoterminowych i dokumentów pobytowych (rozporządzenie w sprawie VIS);**
- 2) Straż Graniczna może dokonać wglądu do danych VIS z poziomu EES w celach, o których mowa w art. 17a ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany informacji pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, wiz długoterminowych i dokumentów pobytowych (rozporządzenie w sprawie VIS).>**

Art. 7. 1. Uprawnienie do pośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu wglądu do danych VIS przysługuje sądowi,

¹¹⁾ Dodany art. 6a wejdzie w życie z dniem określonym w decyzji Komisji Europejskiej, zgodnie z art. 66 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiającego system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określającego warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniającego konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011.

prokuraturze, Policji, Straży Granicznej, Służbie Celno-Skarbowej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Ochrony Państwa, 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;
- 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 Celno-Skarbowej – Szef Krajowej Administracji Skarbowej;
- 4) Agencji Bezpieczeństwa Wewnętrznego – Szef Agencji Bezpieczeństwa Wewnętrznego;
- 5) Agencji Wywiadu – Szef Agencji Wywiadu;
- 6) Centralnego Biura Antykorupcyjnego – Szef Centralnego Biura Antykorupcyjnego;
- 7) (uchylony)
- 8) Służby Ochrony Państwa – Komendant Służby Ochrony Państwa;
- 9) Służby Kontrwywiadu Wojskowego – Szef Służby Kontrwywiadu Wojskowego;
- 10) Służby Wywiadu Wojskowego – Szef Służby Wywiadu Wojskowego;
- 11) Żandarmerii Wojskowej – Komendant Główny Żandarmerii Wojskowej.

<3.¹²⁾ Pośredni dostęp do danych VIS dla podmiotów wymienionych w ust. 1 w przypadku realizowania wniosku o dostęp do danych EES, o którym mowa

¹²⁾ Dodany ust. 3 w art. 7 wejdzie w życie z dniem określonym w decyzji Komisji Europejskiej, zgodnie z art. 66 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiającego system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określającego warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniającego konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011.

w art. 4 ust. 5 ustawy z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu (Dz. U. poz. 1688), jest realizowany przez centralny punkt dostępu, którym jest Komendant Główny Straży Granicznej.>

Rozdział 3

Ochrona danych osobowych oraz odpowiedzialność za niezgodne z prawem działanie lub zaniechanie związane z przetwarzaniem danych

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

Art. 9. Prezes Urzędu Ochrony Danych Osobowych w przypadkach, o których mowa w art. 44 ust. 6 rozporządzenia 2018/1861 oraz art. 59 ust. 6 rozporządzenia 2018/1862, jest organem uprawnionym do przekazania sprawy Europejskiemu Inspektorowi Ochrony Danych w celu podjęcia działań mediacyjnych.

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

Art. 11. 1. Przetwarzanie danych może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez obowiązku ujawniania faktycznego celu zbierania danych.

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

Art. 12. (uchylony)

Art. 13. (uchylony)

Rozdział 4

Bezpieczeństwo Krajowego Systemu Informatycznego (KSI)

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 Wizowym Systemie Informacyjnym, 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 (KSI) w poprzednim roku kalendarzowym.

Art. 16. 1. Minister właściwy do spraw wewnętrznych sprawuje nadzór nad prawidłowością działania Krajowego Systemu Informatycznego (KSI).

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 (KSI) spełnia wymagania techniczne niezbędne do udziału w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym;
- 3) sprawdzania, czy osoby mające dostęp do Krajowego Systemu Informatycznego (KSI) 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 (KSI);
- 5) sprawdzania, czy jest zapewniona odpowiednia fizyczna ochrona Krajowego Systemu Informatycznego (KSI) przez organy mające do niego bezpośredni dostęp, w szczególności czy nie ma możliwości dostępu osób nieuprawnionych do Krajowego Systemu Informatycznego (KSI).

Art. 17. 1. Minister właściwy do spraw wewnętrznych, przed uruchomieniem Krajowego Systemu Informatycznego (KSI), jest uprawniony do sprawdzenia gotowości do prawidłowej eksploatacji Krajowego Systemu Informatycznego (KSI) w ramach poszczególnych organów uprawnionych do bezpośredniego dostępu.

2. W przypadku stwierdzenia braku gotowości do prawidłowej eksploatacji Krajowego Systemu Informatycznego (KSI) w ramach poszczególnych organów uprawnionych do bezpośredniego dostępu minister właściwy do spraw wewnętrznych jest uprawniony do wstrzymania uruchomienia Krajowego Systemu Informatycznego (KSI) w ramach organu, w przypadku którego stwierdzono nieprawidłowości.

Art. 18. W przypadku stwierdzenia nieprawidłowości działania Krajowego Systemu Informatycznego (KSI) 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 (KSI) 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 (KSI) w ramach danego organu;
- 3) zlecać sporządzanie ekspertyz i opinii;
- 4) żądać zablokowania bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) do czasu usunięcia stwierdzonych nieprawidłowości.

Art. 20. W przypadku stwierdzenia nieprawidłowości działania Krajowego Systemu Informatycznego (KSI) 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, warunki techniczne, sposób i tryb dokonywania wpisów danych SIS oraz tworzenia odsyłaczy pomiędzy wpisami w Systemie Informacyjnym Schengen, a także sposób i tryb aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (KSI), 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 (KSI) jako krajowego interfejsu Wizowego Systemu Informacyjnego, w tym sposób dokonywania wpisów danych VIS, a także wglądu do danych VIS, mając na względzie prawidłowe

wykonanie przez Rzeczpospolitą Polską zobowiązań wynikających z udziału w Wizowym Systemie Informacyjnym.

Art. 22. 1. Organy uprawnione zgodnie z art. 3 ust. 2 do dokonania wpisu danych SIS za pośrednictwem centralnego organu technicznego KSI kierują wnioski 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 i 3 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 przetwarzania danych SIS.

Art. 23. Organy, o których mowa w art. 4, w przypadku stwierdzenia, że przetwarzane przez te organy dane SIS są nieprawidłowe, niezwłocznie informują o tym biuro SIRENE w celu weryfikacji prawidłowości tych danych SIS zgodnie z art. 44 ust. 5 rozporządzenia 2018/1861 oraz art. 59 ust. 5 rozporządzenia 2018/1862.

Art. 24. Organ uprawniony do przetwarzania danych poprzez Krajowy System Informatyczny (KSI) jest obowiązany stosować odpowiednie procedury kontrolne wskazujące działania podejmowane w ramach danego organu mające na celu zapewnienie zgodności przetwarzania danych z obowiązującymi przepisami.

Art. 25. 1. Organ uprawniony do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI) jest obowiązany do szkolenia wszystkich osób, które mają realizować to uprawnienie, w zakresie użytkowania Systemu Informacyjnego Schengen i Wizowego Systemu Informacyjnego, bezpieczeństwa i jakości danych, praw podstawowych oraz procedur regulujących przetwarzanie danych.

2. Odbycie szkolenia przed przyznaniem upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez

Krajowy System Informatyczny (KSI) stanowi warunek nadania tego upoważnienia (szkolenie dostępowe). Odbycie szkolenia po przyznaniu upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI) (szkolenia okresowe) następuje zgodnie z terminami określonymi przez organ uprawniony.

3. Centralny organ techniczny KSI na podstawie wystawionego przez organ upoważnienia dla użytkownika indywidualnego do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI) nadaje uprawnienie użytkownikowi indywidualnemu do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI), wydając w tym celu osobisty i niepowtarzalny identyfikator użytkownika indywidualnego, a także prowadzi ewidencję tych użytkowników.

4. Upoważnienie, o którym mowa w ust. 3, zawiera:

- 1) imię i nazwisko użytkownika indywidualnego;
- 2) numer PESEL użytkownika indywidualnego;
- 3) zakres przyznanych użytkownikowi indywidualnemu uprawnień;
- 4) okres, na który przyznaje się użytkownikowi indywidualnemu uprawnienia;
- 5) oświadczenie użytkownika indywidualnego o zobowiązaniu do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem;
- 6) nazwę organu uprawnionego do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI).

5. Centralny organ techniczny KSI cofa uprawnienie użytkownikowi indywidualnemu do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI) na podstawie pisemnego wniosku organu, który wystawił upoważnienie dla użytkownika indywidualnego, zawierającego:

- 1) imię i nazwisko użytkownika indywidualnego;
- 2) numer PESEL użytkownika indywidualnego;
- 3) nazwę organu uprawnionego do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI).

6. Organ, o którym mowa w art. 3 ust. 1 i art. 4 ust. 1, upoważnia użytkownika końcowego do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI), a także prowadzi ewidencję tych użytkowników.

7. Upoważnienie, o którym mowa w ust. 6, zawiera:

- 1) imię i nazwisko użytkownika końcowego;
- 2) numer PESEL użytkownika końcowego;
- 3) zakres przyznanego użytkownikowi końcowemu upoważnienia;
- 4) okres, na który przyznaje się użytkownikowi końcowemu upoważnienie.

8. Upoważnienie dla użytkownika końcowego może zawierać dane inne niż wymienione w ust. 7, wyłącznie jeżeli są one niezbędne do upoważnienia użytkownika końcowego do systemu teleinformatycznego użytkownika instytucjonalnego.

9. Do upoważnienia dla użytkownika końcowego należy dołączyć oświadczenie użytkownika końcowego o zobowiązaniu do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem.

10. Ewidencja, o której mowa w ust. 3, zawiera elementy wymienione w ust. 4 pkt 1–4 oraz datę nadania lub cofnięcia uprawnienia. Ewidencja, o której mowa w ust. 6, zawiera elementy wymienione w ust. 7 i 8 oraz datę nadania lub cofnięcia upoważnienia.

11. Minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii Prezesa Urzędu Ochrony Danych Osobowych, określi, w drodze rozporządzenia, sposób przeprowadzania szkoleń w zakresie określonym w ust. 1, ze szczególnym uwzględnieniem zasad dotyczących ochrony danych osobowych oraz przetwarzania danych, w tym określanych w aktach wykonawczych Komisji Europejskiej przyjętych na podstawie rozporządzenia 2018/1860, rozporządzenia 2018/1861 oraz rozporządzenia 2018/1862, a także kwalifikacje osób uprawnionych do przeprowadzania tych szkoleń, mając na uwadze konieczność zapewnienia możliwości pełnego korzystania z funkcji Systemu Informacyjnego Schengen i Wizowego Systemu Informacyjnego w zakresie przyznanego dostępu.

12. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb nadania dostępu do Krajowego Systemu Informatycznego (KSI)

oraz tryb cofania tego dostępu, sposób przydzielania osobom uprawnionym osobistych i niepowtarzalnych identyfikatorów użytkownika indywidualnego, jak również sposób prowadzenia ewidencji użytkowników końcowych oraz użytkowników indywidualnych, a także wzór upoważnienia dla użytkownika indywidualnego do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI), przy uwzględnieniu konieczności zapewnienia bezpieczeństwa i ochrony przetwarzania danych poprzez Krajowy System Informatyczny (KSI).

Rozdział 5

Centralny organ techniczny KSI

Art. 26. 1. Organem odpowiedzialnym za system krajowy N.SIS jest centralny organ techniczny KSI.

2. Do zadań centralnego organu technicznego KSI należy:

- 1) utworzenie, zapewnienie funkcjonowania, utrzymanie i dalsze rozwijanie Krajowego Systemu Informatycznego (KSI);
- 2) zapewnienie sprawnego działania i bezpieczeństwa Systemu Informacyjnego Schengen w ramach systemu krajowego N.SIS.

Art. 27. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 2, centralny organ techniczny KSI jest obowiązany do:

- 1) przestrzegania obowiązujących protokołów i procedur technicznych w celu zapewnienia kompatybilności Krajowego Systemu Informatycznego (KSI) z systemem centralnym SIS oraz Centralnym Wizowym Systemem Informacyjnym;
- 2) zapewnienia, aby dane SIS przechowywane w kopii krajowej były, dzięki automatycznym aktualizacjom, identyczne i spójne z danymi przechowywanymi w systemie centralnym SIS oraz aby wyszukiwanie przeprowadzone w kopii krajowej prowadziło do wyniku równoważnego wynikowi wyszukiwania w bazie danych systemu centralnego SIS;
- 3) realizacji zadań wskazanych w art. 10 ust. 1 rozporządzenia 2018/1861 oraz art. 10 ust. 1 rozporządzenia 2018/1862;
- 4) umożliwienia organom, o których mowa w art. 3 i art. 4, oraz biuru SIRENE przetwarzania danych SIS poprzez Krajowy System Informatyczny (KSI), w szczególności przez zapewnienie im niezakłóconej dostępności danych SIS,

oraz udzielania tym organom niezbędnych informacji do prawidłowego wykonywania przez nie zadań w zakresie uczestnictwa w Systemie Informacyjnym Schengen;

- 5) umożliwienia organom, o których mowa w art. 5–7, przetwarzania danych VIS poprzez Krajowy System Informatyczny (KSI) oraz udzielania tym organom niezbędnych informacji do prawidłowego wykonywania przez te organy zadań w zakresie uczestnictwa w Wizowym Systemie Informacyjnym;
- 6) przekazywania organowi zarządzającemu systemem centralnym SIS wykazu organów, o których mowa w art. 3 ust. 1 i art. 4 ust. 1, oraz zmian w tym zakresie;
- 7) przekazywania Komisji Europejskiej listy organów, o których mowa w art. 5–7;
- 8) współpracy z jednostką krajową Europolu w zakresie udzielania zgody na dostęp Agencji Unii Europejskiej do spraw Współpracy Organów Ścigania (Europol) do danych VIS;
- 9) zapewnienia rejestrowania wszystkich przypadków, w których uzyskano dostęp do danych lub wykorzystano dane w inny sposób poprzez Krajowy System Informatyczny (KSI);
- 10) współdziałania z organami, o których mowa w art. 3 ust. 1, w celu zapewnienia zgodności z prawem, dokładności i aktualności wpisów danych SIS.

2. Centralnemu organowi technicznemu KSI powierza się sprawozdawczość związaną z funkcjonowaniem Krajowego Systemu Informatycznego (KSI), w tym prowadzenie statystyk określonych w art. 39 ust. 6 rozporządzenia 2018/1861 oraz art. 53 ust. 8 i art. 54 ust. 6 rozporządzenia 2018/1862.

Art. 28. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, szczegółowy sposób rejestrowania przypadków, o których mowa w art. 27 ust. 1 pkt 9, mając na względzie bezpieczeństwo i ochronę danych przetwarzanych poprzez Krajowy System Informatyczny (KSI).

Art. 29. 1. Centralny organ techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego (KSI), jest obowiązany poinformować ministra właściwego do spraw wewnętrznych o gotowości Krajowego Systemu Informatycznego (KSI) do uruchomienia.

2. Minister właściwy do spraw wewnętrznych, po uzyskaniu informacji, o której mowa w ust. 1, przeprowadza kontrolę w zakresie spełniania przez Krajowy System

Informatyczny (KSI) wymogów określonych w art. 9 ust. 1 i 2 rozporządzenia 2018/1861 oraz art. 9 ust. 1 i 2 rozporządzenia 2018/1862.

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 (KSI) wymogów określonych w art. 9 ust. 1 i 2 rozporządzenia 2018/1861 oraz art. 9 ust. 1 i 2 rozporządzenia 2018/1862, a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym (KSI) przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej.

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

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

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

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

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

5) zlecać sporządzanie ekspertyz i opinii.

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

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

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

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

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

Art. 33. Uruchomienie Krajowego Systemu Informatycznego (KSI) 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. 1. W przypadku dokonywania zmian w Krajowym Systemie Informatycznym (KSI) po jego uruchomieniu, mających wpływ na bezpieczeństwo w zakresie, o którym mowa w art. 10 rozporządzenia 2018/1861 oraz

art. 10 rozporządzenia 2018/1862, centralny organ techniczny KSI jest obowiązany przed wdrożeniem tych zmian do uzyskania pisemnej opinii ministra właściwego do spraw wewnętrznych w zakresie spełnienia przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 4 i art. 9 rozporządzenia 2018/1861 oraz art. 4 i art. 9 rozporządzenia 2018/1862, a także opinii Prezesa Urzędu Ochrony Danych Osobowych.

2. W celu wydania opinii minister właściwy do spraw wewnętrznych przeprowadza kontrolę w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów, o których mowa w ust. 1.

3. Po przeprowadzeniu kontroli minister właściwy do spraw wewnętrznych przedstawia centralnemu organowi technicznemu KSI pisemną opinię, o której mowa w ust. 1, a w przypadku stwierdzenia nieprawidłowości w Krajowym Systemie Informatycznym (KSI) przekazuje centralnemu organowi technicznemu KSI zalecenia pokontrolne w formie pisemnej. W przypadku przekazania zaleceń pokontrolnych przepis art. 31 stosuje się odpowiednio do centralnego organu technicznego KSI.

4. W przypadku niezgłoszenia przez centralny organ techniczny KSI zastrzeżeń, jak również w przypadku nieuwzględnienia zastrzeżeń przez ministra właściwego do spraw wewnętrznych, centralny organ techniczny KSI jest obowiązany wykonać zalecenia pokontrolne, a następnie wystąpić z wnioskiem do ministra właściwego do spraw wewnętrznych o przeprowadzenie kontroli, o której mowa w ust. 2.

5. Uzyskanie opinii Prezesa Urzędu Ochrony Danych Osobowych, o której mowa w ust. 1, następuje w zakresie i w trybie określonych w art. 30–32.

Rozdział 6

Biuro SIRENE

Art. 35. 1. W ramach struktury Komendy Głównej Policji wyznacza się komórkę organizacyjną będącą biurem SIRENE, zapewniającą w szczególności wymianę informacji uzupełniających w trybie i zgodnie z zasadami określonymi w aktach wykonawczych przyjętych przez Komisję Europejską na podstawie art. 8 ust. 4 rozporządzenia 2018/1861 oraz art. 8 ust. 4 rozporządzenia 2018/1862.

2. Biuro SIRENE, w celu realizacji zadań, posiada bezpośredni dostęp do Krajowego Systemu Informatycznego (KSI).

3. W ramach biura SIRENE współdziałają funkcjonariusze i pracownicy Policji i Straży Granicznej, którzy wspólnie realizują zadania określone w ust. 1.

Szczegółowy zakres i podział zadań oraz sposoby współdziałania określa porozumienie zawarte pomiędzy Komendantem Głównym Straży Granicznej a Komendantem Głównym Policji.

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 oraz zapewnienia łatwego, bezpośredniego lub pośredniego dostępu do wszelkich stosownych informacji i do baz danych w zakresie dokonywanych przez te organy wpisów.

2. Obowiązek, o którym mowa w ust. 1, dotyczy w szczególności bezzwłocznego przekazywania do biura SIRENE, w związku z dokonaniem poprzez Krajowy System Informatyczny (KSI) 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. z 2021 r. poz. 1697 oraz z 2023 r. poz. 547), a także przekazywania odpowiednio wszystkich istotnych informacji w odniesieniu do wpisów dokonywanych zgodnie z art. 3 ust. 1 od momentu utworzenia wpisu zgodnie z zakresem określonym w aktach wykonawczych przyjętych przez Komisję Europejską na podstawie art. 8 ust. 4 rozporządzenia 2018/1861 oraz art. 8 ust. 4 rozporządzenia 2018/1862.

Rozdział 7

Zmiany w przepisach obowiązujących

Art. 38–42. (pominięte)

Rozdział 8

Przepisy przejściowe i końcowe

Art. 43. Centralny organ techniczny KSI jest obowiązany do utworzenia oraz uruchomienia Krajowego Systemu

Informatycznego (KSI) w terminie do dnia 1 września 2007 r.

Art. 44. Osoby mające dostęp do Krajowego Systemu Informatycznego (KSI) 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. (pominięty)

Art. 46. Ustawa wchodzi w życie z dniem ogłoszenia¹³⁾, 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 Wizowego Systemu Informacyjnego w Rzeczypospolitej Polskiej;
- 2) (uchylony)
- 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. poz. 864).

¹³⁾ Ustawa została ogłoszona w dniu 14 września 2007 r.