**TABELA ZGODNOŚCI**

|  |  |
| --- | --- |
| **TYTUŁ PROJEKTU:** | **ustawa o zmianie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym** |
| **TYTUŁ WDRAŻANEGO AKTU PRAWNEGO/ WDRAŻANYCH AKTÓW PRAWNYCH:** | **Rozporządzenie 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** |
|  | |
| **PRZEPISY UNII EUROPEJSKIEJ** | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Jedn.**  **Red.** | **Treść przepisu UE** | **Konieczność wdrożenia**  **T/N** | **Jedn.**  **Red.** | **Treść przepisu/ów projektu** | **Uzasadnienie uwzględnienia  w projekcie przepisów wykraczających poza minimalne wymogi prawa UE** |
| **Rozdział I**  **Przepisy ogólne** | | | | | | |
| **Art. 1**  **Cel** | | | | | | |
|  | **Art. 1** | Artykuł 1  **Cel ogólny SIS**  Celem SIS jest zapewnienie – przy wykorzystaniu informacji przekazywanych za pośrednictwem tego systemu – wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii, w tym utrzymywanie bezpieczeństwa publicznego i porządku publicznego oraz zagwarantowanie bezpieczeństwa na terytorium państw członkowskich, a także zapewnienie stosowania postanowień rozdziału 4 i rozdziału 5 tytułu V części trzeciej TFUE w odniesieniu do przepływu osób na terytorium państw członkowskich. | **T** | Art. 1 pkt 2 lit. d | d) pkt 14a–15a otrzymują brzmienie:  „14a) systemie centralnym SIS – rozumie się przez to system centralny, o którym mowa w art. 4 ust. 1 lit. a rozporządzenia 2018/1861 oraz w art. 4 ust. 1 lit. a rozporządzenia 2018/1862;  15) Systemie Informacyjnym Schengen – rozumie się przez to system informacyjny, o którym mowa w art. 14 rozporządzenia 2018/1861 oraz w **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, o którym mowa w art. 4 ust. 1 lit. b rozporządzenia 2018/1861 oraz w art. 4 ust. 1 lit. b rozporządzenia 2018/1862;”,  . | Wraz z wejściem w życie Rozporządzeń Parlamentu Europejskiego i Rady (UE) 2018/1860, 2018/1861 oraz 2018/1862 nastąpi zmiana podstawy prawnej funkcjonowania Systemu Informacyjnego Schengen, która musi zostać odwzorowana w przepisach krajowych. |
|  | **Art. 2** | Artykuł 2  **Przedmiot**  1. Niniejsze rozporządzenie określa warunki i procedury wprowadzania do SIS i przetwarzania wpisów w SIS dotyczących osób i przedmiotów oraz wymiany informacji uzupełniających i danych dodatkowych w celach związanych ze współpracą policyjną i współpracą wymiarów sprawiedliwości w sprawach karnych.  2. Niniejsze rozporządzenie ustanawia również przepisy dotyczące architektury technicznej SIS, obowiązków państw członkowskich i Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa | **N** |  |  | Artykuł określa zakres regulacji niniejszego rozporządzania. |
|  | **Art. 3** | Artykuł 3  **Definicje**  Na użytek niniejszego rozporządzenia stosuje się następujące definicje: 1) „wpis” oznacza zestaw danych wprowadzonych do SIS, które umożliwiają właściwym organom zidentyfikowanie osoby lub przedmiotu w celu podjęcia konkretnego działania; 2) „informacje uzupełniające” oznaczają informacje, które nie są częścią danych zawartych we wpisach przechowywanych w SIS, ale są związane z wpisami w SIS, i które podlegają wymianie za pośrednictwem biur SIRENE: a) w celu umożliwienia państwom członkowskim wzajemnej konsultacji lub wzajemnego informowania się podczas wprowadzania wpisu; b) w celu umożliwienia podjęcia odpowiedniego działania po uzyskaniu trafienia; c) w przypadku niemożności podjęcia wymaganego działania; d) w przypadku rozwiązywania kwestii jakości danych w SIS; e) w przypadku rozwiązywania kwestii zgodności i priorytetu wpisów; f) w przypadku rozwiązywania kwestii związanych z prawami do dostępu; 3) „dane dodatkowe” oznaczają dane przechowywane w SIS – i związane z wpisami w SIS – które mają być natychmiast dostępne dla właściwych organów, gdy osobę, w odniesieniu do której wprowadzono dane do SIS, zlokalizowano w wyniku wyszukiwania przeprowadzonego w SIS;  4) „dane osobowe” oznaczają dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679; 5) „przetwarzanie danych osobowych” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak gromadzenie, utrwalanie, rejestrowanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie; 6) „dopasowanie” oznacza łączne wystąpienie następujących elementów: a) wyszukiwanie w SIS przeprowadza użytkownik końcowy; b) w wyniku wyszukiwania znaleziono wpis wprowadzony do SIS przez inne państwo członkowskie; oraz c) dane dotyczące wpisu w SIS pasują do danych wprowadzonych na potrzeby wyszukiwania; 7) „trafienie” oznacza dopasowanie, które spełnia następujące kryteria: a) zostało potwierdzone przez: (i) użytkownika końcowego; lub (ii) właściwy organ zgodnie z procedurami krajowymi, w przypadku gdy dane dopasowanie opierało się na porównaniu danych biometrycznych; oraz b) wymagane jest podjęcie dalszych działań; 8) „zastrzeżenie” oznacza zawieszenie ważności wpisu na poziomie krajowym, które można umieścić przy wpisach mających doprowadzić do aresztowania, wpisach dotyczących osób zaginionych i osób narażonych na niebezpieczeństwo oraz wpisach wykorzystywanych do prowadzenia kontroli niejawnych, rozpytań kontrolnych i kontroli szczególnych; 9) „państwo członkowskie dokonujące wpisu” oznacza państwo członkowskie, które wprowadziło wpis do SIS; 10) „wykonujące państwo członkowskie” oznacza państwo członkowskie, które podejmuje lub podjęło wymagane działania po uzyskaniu trafienia; 11) „użytkownik końcowy” oznacza członka personelu właściwego organu uprawnionego do przeprowadzenia wyszukiwania bezpośrednio w CS-SIS, N.SIS lub ich kopii technicznej; 12) „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych lub fizjologicznych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, a mianowicie fotografie, wizerunki twarzy, dane daktyloskopijne i profile DNA; 13) „dane daktyloskopijne” oznaczają dane dotyczące odbitek linii papilarnych palców i odbitek linii papilarnych dłoni, które z powodu ich niepowtarzalnego charakteru i układu cech szczególnych umożliwiają przeprowadzenie dokładnych i dających jednoznaczne wyniki porównań odnośnie do tożsamości danej osoby; 14) „wizerunek twarzy” oznacza cyfrowe obrazy twarzy mające dostateczną rozdzielczość i jakość, aby można je było wykorzystywać na potrzeby zautomatyzowanego dopasowywania biometrycznego; 15) „profil DNA” oznacza kod literowy lub numeryczny reprezentujący zestaw charakterystycznych cech identyfikacyjnych niekodującej części przeanalizowanej próbki ludzkiego DNA, a mianowicie szczególną strukturę molekularną w różnych loci DNA; 16) „przestępstwa terrorystyczne” oznaczają przestępstwa w rozumieniu prawa krajowego, o których mowa w art. 3–14 dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 ( 1 ), lub – w przypadku państw członkowskich niezwiązanych tą dyrektywą – które są równoważne jednemu z przestępstw wymienionych w tej dyrektywie; 17) „zagrożenie dla zdrowia publicznego” oznacza zagrożenie dla zdrowia publicznego zdefiniowane w art. 2 pkt 21 rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/399 ( 2 ). | **T** | Art 1 pkt 2 lit. b  Art. 1 pkt 2 lit. e | lit. b)  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**;”  lit. e)  pkt 18 otrzymuje brzmienie:  „18) przetwarzaniu danych – rozumie się przez to przetwarzanie danych osobowych, o którym mowa w art. 3 pkt 6 rozporządzenia 2018/1861 i art. 3 pkt 5 rozporządzenia 2018/1862, a także jakiekolwiek operacje wykonywane na danych niebędących danymi osobowymi, takie jak: zbieranie, wpisywanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;”;  lit. f)  w pkt 19 kropkę zastępuje się średnikiem i dodaje się pkt 20–27 w brzmieniu:  „20) dopasowaniu danych SIS – rozumie się przez to dopasowanie, o którym mowa w art. 3 pkt 7 rozporządzenia 2018/1861 i **art. 3 pkt 6 rozporządzenia 2018/1862**;  21) tożsamości przywłaszczonej – rozumie się przez to dane wprowadzone do SIS zgodnie z art. 47 rozporządzenia 2018/1861 oraz zgodnie z art. 62 rozporządzenia 2018/1862dotyczące osoby pokrzywdzonej, której tożsamością posługuje się osoba poszukiwana na podstawie wpisu do SIS;  22) odsyłaczu – rozumie się przez to odsyłacz, o którym mowa w art. 48 rozporządzenia 2018/1861 i art. 63 rozporządzenia 2018/1862, utworzony w SIS pomiędzy co najmniej dwoma wpisami;  23) danych biometrycznych – rozumie się przez to dane, o których mowa w art. 3 pkt 13 rozporządzenia 2018/1861 i **art. 3 pkt 12 rozporządzenia 2018/1862**;  24) danych daktyloskopijnych – rozumie się przez to dane, o których mowa w art. 3 pkt 14 rozporządzenia 2018/1861 i **art. 3 pkt 13 rozporządzenia 2018/1862**;  25) użytkowniku indywidualnym - należy przez to rozumieć 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;  26) użytkowniku instytucjonalnym - należy przez to rozumieć organ uprawniony do dostępu i współpracy z Krajowym Systemem Informatycznym (KSI) za pośrednictwem własnego systemu teleinformatycznego;  27) użytkowniku końcowym - należy przez to rozumieć osobę fizyczną upoważnioną do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI) za pośrednictwem systemu teleinformatycznego użytkownika instytucjonalnego.”;  3) użyte w art. 2 pkt 13, art. 5 ust. 2 pkt 5 i ust. 3, art. 6 pkt 4-7 oraz art. 11 ust. 2 w różnym przypadku i liczbie wyrazy „Państwo Członkowskie” zastępuje się użytymi w odpowiednim przypadku i liczbie wyrazami „państwo członkowskie”; | Zapewnienie spójności słownika pojęć w art. 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym z Definicjami znajdującymi się w art. 2 Rozporządzenia 2018/1860 i art. 3 Rozporządzenia 2018/1861.  Zmiany dotyczą pojęć nowych niestosowanych bezpośrednio (związanych z funkcjonowaniem systemu SIS). Art. 2 pkt 18 ma na celu zdefiniowanie pojęcia „przetwarzania danych” przy zastosowaniu odesłania do art. 3 pkt 6 rozporządzenia 2018/1861 i art. 3 pkt 5 rozporządzenia 2018/1862, które to przepisy definiują „przetwarzanie danych osobowych”. Powyższe podyktowane jest konsekwentnym realizowaniem w projekcie założenia o potrzebie zapewnienia spójności przepisów krajowych z przepisami UE. Aktualnie odstąpiono też od odwołania w definicji do przepisów regulujących przetwarzanie danych osobowych z uwagi na brak znaczenia normatywnego takiego zapisu. Organy uprawnione zgodnie z projektem do przetwarzania danych SIS działają bowiem z mocy prawa w reżimie prawnym wyznaczonym przepisami ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczeniem przestępczości (Dz. U. z 2019 r. poz. 125) oraz rozporządzenia 2016/679 (vide art. 288 zdanie trzecie Traktatu o funkcjonowaniu Unii Europejskiej). |
|  | **Art. 4** | Artykuł 4  **Architektura techniczna i sposoby funkcjonowania SIS**  1. SIS składa się z: a) systemu centralnego (zwanego dalej „systemem centralnym SIS”) składającego się z: (i) funkcji wsparcia technicznego (CS-SIS), zawierającej bazę danych (zwaną dalej „bazą danych SIS”) oraz wersję zapasową CS-SIS; (ii) jednolitego interfejsu krajowego (NI-SIS); b) systemu krajowego (N.SIS) w każdym państwie członkowskim, składającego się z krajowych systemów danych, które łączą się z systemem centralnym SIS w tym co najmniej jednej krajowej lub wspólnej wersji zapasowej N.SIS; oraz c) infrastruktury łączności pomiędzy CS-SIS, wersją zapasową CS-SIS i NI-SIS (zwanej dalej „infrastrukturą łączności”), która zapewnia zaszyfrowaną wirtualną sieć na potrzeby danych SIS oraz wymiany danych między biurami SIRENE, o której mowa w art. 7 ust. 2. N.SIS, o którym mowa w lit. b), może zawierać plik danych (zwany dalej „kopią krajową”), zawierający pełną lub częściową kopię bazy danych SIS. Dwa państwa członkowskie lub większa ich liczba mogą utworzyć w jednym ze swoich N.SIS wspólną kopię, z której mogą wspólnie korzystać. Taka wspólna kopia uważana jest za kopię krajową każdego z tych państw członkowskich. Ze wspólnej wersji zapasowej N.SIS, o której mowa w lit. b), mogą wspólnie korzystać dwa państwa członkowskie lub większa ich liczba. W takich przypadkach wspólną wersję zapasową N.SIS traktuje się jako wersję zapasową N.SIS każdego z tych państw członkowskich. Aby zapewnić użytkownikom końcowym niezakłóconą dostępność, istnieje możliwość jednoczesnego korzystania z N.SIS i jego wersji zapasowej. Państwa członkowskie zamierzające utworzyć wspólną kopię lub wspólną wersję zapasową N.SIS, z których mogą wspólnie korzystać, uzgadniają na piśmie swoje odpowiednie obowiązki. O uzgodnieniach tych informują one Komisję. Infrastruktura łączności wspiera i pomaga zapewnić niezakłóconą dostępność SIS. Obejmuje ona redundantne i rozdzielne ścieżki dla połączeń między CS-SIS i wersją zapasową CS-SIS, a także redundantne i rozdzielne ścieżki dla połączeń między każdym krajowym punktem dostępu do sieci SIS oraz CS-SIS i wersją zapasową CS-SIS. 2. Państwa członkowskie wprowadzają, aktualizują, usuwają i wyszukują dane SIS, korzystając ze swoich N. SIS. Państwa członkowskie korzystające z częściowej lub pełnej krajowej kopii lub częściowej lub pełnej wspólnej kopii udostępniają tę kopię do celów przeprowadzania zautomatyzowanych wyszukiwań na terytorium każdego z tych państw członkowskich. Częściowa krajowa lub wspólna kopia zawiera co najmniej dane wymienione w art. 20 ust. 3 lit. a)–v). Przeszukiwanie plików danych przechowywanych w N.SIS innych państw członkowskich nie jest możliwe, z wyjątkiem sytuacji, gdy dotyczy to wspólnych kopii. 3. CS-SIS wykonuje techniczne funkcje nadzorcze i administracyjne i posiada wersję zapasową CS-SIS, która jest w stanie zapewnić wszystkie funkcje głównego CS-SIS w przypadku jego awarii. CS-SIS i wersja zapasowa CS-SIS znajdują się w dwóch centrach technicznych eu-LISA. 4. eu-LISA wdraża rozwiązania techniczne mające na celu zwiększenie niezakłóconej dostępności SIS poprzez jednoczesne funkcjonowanie CS-SIS i wersji zapasowej CS-SIS, o ile taka wersja zapasowa CS-SIS jest w stanie zagwarantować funkcjonowanie SIS w przypadku awarii, albo poprzez duplikację systemu lub jego komponentów. Niezależnie od wymogów proceduralnych określonych w art. 10 rozporządzenia (UE) 2018/1726, eu-LISA przygotuje, nie później niż dnia 28 grudnia 2019 r., opracowanie dotyczące opcji w zakresie rozwiązań technicznych, zawierające niezależną ocenę skutków oraz analizę kosztów i korzyści. 5. Jeżeli jest to konieczne w wyjątkowych okolicznościach, eu-LISA może przygotować, jako tymczasowe rozwiązanie, dodatkową kopię bazy danych SIS. 6. CS-SIS zapewnia usługi niezbędne do wprowadzania i przetwarzania danych SIS, w tym do prowadzenia wyszukiwań w bazie danych SIS. CS-SIS zapewnia państwom członkowskim korzystającym z krajowej lub wspólnej kopii: a) aktualizację kopii krajowych w trybie online; b) synchronizację i spójność kopii krajowych z bazą danych SIS; oraz c) czynności związane z inicjalizacją i odtwarzaniem kopii krajowych. 7. CS-SIS zapewnia niezakłóconą dostępność. | **T** | Art. 1 pkt 2 lit. d  Art. 4 ust. 1 pkt 12 | pkt 2 lit. d)  pkt 14a–15a otrzymują brzmienie:  „14a) systemie centralnym SIS – rozumie się przez to system centralny, o którym mowa w art. 4 ust. 1 lit. a rozporządzenia 2018/1861 oraz w **art. 4 ust. 1 lit. a rozporządzenia 2018/1862**;  15) Systemie Informacyjnym Schengen – rozumie się przez to system informacyjny, o którym mowa w art. 14 rozporządzenia 2018/1861 oraz **w 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, o którym mowa w art. 4 ust. 1 lit. b rozporządzenia 2018/1861 oraz w **art. 4 ust. 1 lit. b rozporządzenia 2018/1862**;”,  Ust 12:  użyte w art. 26 ust. 1 i art. 26 ust. 2 pkt 2 w różnym przypadku wyrazy „system krajowy N.SIS II” zastępuje się użytymi w odpowiednim przypadku wyrazami „**system krajowy N.SIS**”; | Rozporządzenia 2018/1860, 2018/1861 oraz 2018/1862 zmieniają nazewnictwo niektórych pojęć dotyczących architektury oraz sposobu funkcjonowania systemu SIS, które muszą zostać odwzorowane w ustawie o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym.  Art. 4 ust. 3-7 nie wymagają transpozycji. |
|  | **Art. 5** | Artykuł 5  **Koszty**  1. Koszty funkcjonowania, utrzymania i dalszego rozwijania systemu centralnego SIS i infrastruktury łączności są pokrywane z budżetu ogólnego Unii. Koszty te obejmują także koszty prac przeprowadzanych w odniesieniu do CS-SIS, w celu zapewnienia usług, o których mowa w art. 4 ust. 6.  2. Koszty utworzenia, funkcjonowania, utrzymania i dalszego rozwijania każdego N.SIS ponosi odnośne państwo członkowskie. | **N** |  |  | Koszty rozwoju i utrzymanie centralnej części systemu co jest realizowane przez Agencję eu-LISA. |
|  | **Art. 6** | Artykuł 6  **Systemy krajowe**  Każde państwo członkowskie odpowiada za utworzenie, funkcjonowanie, utrzymanie i dalsze rozwijanie swojego N.SIS oraz za przyłączenie go do NI-SIS. Każde państwo członkowskie odpowiada za zapewnienie użytkownikom końcowym niezakłóconej dostępności danych SIS. Każde państwo członkowskie przekazuje swoje wpisy za pośrednictwem swojego N.SIS. | **T** | Art. 1 pkt 13  Art. 1 pkt 14 | 13)  w art. 26 w ust. 2 pkt 1 otrzymuje brzmienie:  „1) utworzenie, zapewnienie funkcjonowania, utrzymanie i dalsze rozwijanie Krajowego Systemu Informatycznego (KSI);”;  14)  art. 27 otrzymuje brzmienie:  „Art. 27. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 2, centralny organ techniczny KSI jest obowiązany do:  (…)  4) umożliwienia organom uprawnionym, wskazanym w art. 3–4, przetwarzania danych SIS poprzez Krajowy System Informatyczny (KSI), w szczególności poprzez 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; | Zgodnie z ustawą o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym:  - Rolę urzędu N.SIS pełni centralny organ techniczny KSI – komendant Główny Policji (art. 2 ust. 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym). |
|  | **Art. 7** | Artykuł 7  **Urząd N.SIS i biuro SIRENE**  1. Każde państwo członkowskie wyznacza organ (zwany dalej „urzędem N.SIS”), który na szczeblu centralnym odpowiada za N.SIS tego państwa. Organ ten odpowiada za sprawne funkcjonowanie i bezpieczeństwo N.SIS, zapewnia właściwym organom dostęp do SIS i stosuje niezbędne środki, aby zapewnić przestrzeganie niniejszego rozporządzenia. Odpowiada on za zapewnienie, aby wszystkie funkcje SIS były we właściwy sposób udostępniane użytkownikom końcowym.  2. Każde państwo członkowskie wyznacza organ krajowy, który działa przez 24 godziny na dobę, 7 dni w tygodniu, oraz zapewnia wymianę i dostępność wszelkich informacji uzupełniających (zwany „biurem SIRENE”) zgodnie z podręcznikiem SIRENE. Każde biuro SIRENE pełni w swoim państwie członkowskim rolę jedynego punktu kontaktowego właściwego do wymiany informacji uzupełniających dotyczących wpisów oraz do ułatwiania podejmowania wymaganych działań, w przypadku gdy do SIS wprowadzono wpisy dotyczące osób lub przedmiotów, które następnie zostały zlokalizowane po uzyskaniu trafienia. Każde biuro SIRENE musi mieć, zgodnie z prawem krajowym, łatwy bezpośredni lub pośredni dostęp do wszelkich stosownych informacji krajowych, w tym krajowych baz danych i wszelkich informacji dotyczących wpisów swojego państwa członkowskiego, a także do fachowego doradztwa, tak by móc podejmować działania w odpowiedzi na wnioski o informacje uzupełniające w szybki sposób i w terminach określonych w art. 8. Biura SIRENE koordynują weryfikację jakości informacji wprowadzonych do SIS. W tym celu mają dostęp do danych przetwarzanych w SIS.  3. Państwa członkowskie przekazują eu-LISA informacje o swoim urzędzie N.SIS i swoim biurze SIRENE. eu-LISA publikuje wykaz urzędów N.SIS i biur SIRENE wraz z wykazem, o którym mowa w art. 56 ust. 7. | **T** | Art. 1 pkt 18 | 18) w art. 35 ust. 1 otrzymuje brzmienie:  „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 na podstawie art. 8 ust. 4 rozporządzenia 2018/1861 oraz **art. 8 ust. 4 rozporządzenia 2018/1862**.”; | Zgodnie z ustawą o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym:  - Rolę urzędu N.SIS pełni centralny organ techniczny KSI – komendant Główny Policji (art. 2 ust. 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym)  - Biuro SIRENE działa w strukturach Komendy Głównej Policji (Rozdział 5 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym).  Nowelizacja aktualizuje podstawę prawną działania Biura SIRENE.  Art. 35 ust. 1 ustawy polega na powiązaniu odwołania z aktualnymi przepisami prawa unijnego dotyczącymi SIS - projekt odwołuje się w ww. zakresie do zasad określonych szczegółowo w aktach wykonawczych przyjętych przez Komisję Europejską na podstawie art. 8 ust. 4 rozporządzenia 2018/1861, tj. decyzji wykonawczej KE z dnia 18 listopada 2021 r. określającej szczegółowe zasady dotyczące zadań biur SIRENE oraz zasady wymiany informacji uzupełniających dotyczących wpisów w Systemie Informacyjnym Schengen w dziedzinie odpraw granicznych i powrotów („Podręcznik SIRENE – Granice i powrót”) oraz art. 8 ust. 4 rozporządzenia 2018/1862, tj. decyzji wykonawczej KE z dnia 18 listopada 2021 r. określającej szczegółowe zasady dotyczące zadań biur SIRENE oraz zasady wymiany informacji uzupełniających dotyczących wpisów w Systemie Informacyjnym Schengen w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych („Podręcznik SIRENE – Policja”).  W zakresie art. 7 ust. 3 rozporządzenie nie wymaga transpozycji. |
|  | **Art. 8** | Artykuł 8  **Wymiana informacji uzupełniających**  1. Wymiana informacji uzupełniających prowadzona jest zgodnie z zasadami zawartymi w podręczniku SIRENE, i za pośrednictwem infrastruktury łączności. Państwa członkowskie zapewniają niezbędne zasoby techniczne i ludzkie w celu zapewnienia ciągłej dostępności oraz terminowej i skutecznej wymiany informacji uzupełniających. W przypadku gdy infrastruktura łączności jest niedostępna, państwa członkowskie wykorzystują inne odpowiednio zabezpieczone środki techniczne do prowadzenia wymiany informacji uzupełniających. Wykaz odpowiednio zabezpieczonych środków technicznych ustanawia się w podręczniku SIRENE.  2. Informacje uzupełniające są wykorzystywane wyłącznie w celu, w którym zostały przekazane zgodnie z art. 64, chyba że uzyskana zostanie uprzednia zgoda państwa członkowskiego dokonującego wpisu na inne wykorzystanie. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/69  3. Biura SIRENE realizują swoje zadanie w sposób szybki i skuteczny, w szczególności udzielając odpowiedzi na wniosek o informacje uzupełniające w jak najszybszym terminie, lecz nie później niż 12 godzin od jego otrzymania. W przypadku wpisów dotyczących przestępstw terrorystycznych, wpisów dotyczących osób poszukiwanych w celu ich aresztowania i wydania lub aresztowania i ekstradycji oraz w przypadkach wpisów dotyczących dzieci, o których mowa w art. 32 ust. 1 lit. c), biura SIRENE natychmiast podejmują działania. Wnioski o informacje uzupełniające mające najwyższy priorytet oznacza się w formularzach SIRENE jako „PILNE”, podając przy tym uzasadnienie pilnego charakteru danej sprawy.  4. Komisja przyjmuje akty wykonawcze w celu określenia szczegółowych zasad dotyczących zadań biur SIRENE wynikających z niniejszego rozporządzenia oraz zasad wymiany informacji uzupełniających – w formie podręcznika zatytułowanego „Podręcznik SIRENE”. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 18 | 18) w art. 35 ust. 1 otrzymuje brzmienie:  „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 na podstawie **art. 8 ust. 4 rozporządzenia 2018/1861 oraz art. 8 ust. 4 rozporządzenia 2018/1862.”;** | Biuro SIRENE działa w strukturach Komendy Głównej Policji (Rozdział 5 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym).  Nowelizacja aktualizuje podstawę prawną działania Biura SIRENE.  Art. 8 ust. 4 nie wymaga transpozycji. |
|  | **Art. 9** | Artykuł 9  **Zgodność pod względem technicznym i funkcjonalnym**  1. Tworząc swój N.SIS, każde państwo członkowskie przestrzega wspólnych norm, protokołów i procedur technicznych mających na celu zapewnienie kompatybilności jego N.SIS z systemem centralnym SIS na potrzeby szybkiego i skutecznego przesyłania danych.  2. Jeżeli państwo członkowskie korzysta z kopii krajowej, zapewnia ono – wykorzystując usługi zapewniane przez CS-SIS i dzięki zautomatyzowanym aktualizacjom, o których mowa w art. 4 ust. 6 – by dane przechowywane w kopii krajowej były identyczne i spójne z danymi w bazie danych SIS oraz by wyszukiwanie przeprowadzane w jego kopii krajowej prowadziło do wyniku równoważnego wynikowi wyszukiwania w bazie danych SIS.  3. Użytkownicy końcowi otrzymują dane niezbędne do wykonania swoich zadań, w szczególności i w razie potrzeby, wszelkie dostępne dane umożliwiające identyfikację osoby, której dane dotyczą, oraz podjęcie wymaganego działania.  4. Państwa członkowskie i eu-LISA przeprowadzają regularne testy w celu zweryfikowania technicznej zgodności kopii krajowych, o której mowa w ust. 2. Wyniki tych testów są uwzględniane jako część mechanizmu ustanowionego na mocy rozporządzenia Rady (UE) nr 1053/2013.  5. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania wspólnych norm, protokołów i procedur technicznych, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 16  Art. 1 pkt 17 | 16) w art. 29 ust. 2 i 3 otrzymują brzmienie:  „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 w **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 w **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.”;  17) w art. 34 ust. 1 otrzymuje brzmienie:  „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.”; | Aktualizacja zasad zapewnienia zgodności N.SIS pod względem technicznym i funkcjonalnym i jej oceny.  Art. 9 ust. 4 i 5 nie wymagają transpozycji. |
|  | **Art. 10** | Artykuł 10  **Bezpieczeństwo – państwa członkowskie**  1. W odniesieniu do swojego N.SIS każde państwo członkowskie przyjmuje niezbędne środki, obejmujące plan bezpieczeństwa, plan ciągłości działania i plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, aby: a) zapewnić fizyczną ochronę danych, w tym poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej; b) uniemożliwić osobom nieuprawnionym dostęp do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury); c) zapobiegać nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych); d) zapobiegać nieuprawnionemu wprowadzaniu danych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania); e) zapobiegać korzystaniu z systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników); f) zapobiegać nieuprawnionemu przetwarzaniu danych w SIS oraz wszelkiemu nieuprawnionemu zmienianiu lub usuwaniu danych przetwarzanych w SIS (kontrola wprowadzania danych); g) zapewnić, by osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadanym przez nie uprawnieniem, wyłącznie pomocą indywidualnych i niepowtarzalnych identyfikatorów użytkownika oraz poufnego trybu dostępu (kontrola dostępu do danych);  h) zapewnić, by wszystkie organy mające prawo dostępu do SIS lub do infrastruktury przetwarzania danych stworzyły profile z opisem funkcji i zadań osób, które są uprawnione do dostępu do danych oraz do ich wprowadzania, aktualizowania, usuwania i wyszukiwania, oraz by profile te były niezwłocznie udostępniane organom nadzorczym, o których mowa w art. 69 ust. 1, na ich wniosek (profile personelu); i) zapewnić możliwość weryfikacji i stwierdzania, którym podmiotom można przesyłać dane osobowe za pośrednictwem sprzętu do przesyłu danych (kontrola przesyłu danych); j) zapewnić możliwość późniejszej weryfikacji i stwierdzania, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania danych oraz kiedy, przez kogo i w jakim celu (kontrola wprowadzania danych); k) zapobiegać nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas transportu nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu); l) monitorować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie, oraz stosować konieczne środki organizacyjne dotyczące monitorowania wewnętrznego, aby zapewnić przestrzeganie niniejszego rozporządzenia (kontrolowanie własnej działalności); m) zapewnić w razie przerwy w działaniu możliwość przywrócenia normalnego funkcjonowania zainstalowanych systemów (odzyskiwanie); oraz n) zapewnić, by SIS wykonywał właściwie swoje funkcje, by błędy były zgłaszane (niezawodność) i by dane osobowe przechowywane w SIS nie mogły ulec uszkodzeniu w wyniku nieprawidłowego funkcjonowania systemu (integralność).  2. Państwa członkowskie stosują środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do bezpieczeństwa przetwarzania i wymiany informacji uzupełniających, w tym zabezpieczenia pomieszczeń biura SIRENE.  3. Państwa członkowskie stosują środki równoważne środkom, o których mowa w ust. 1 niniejszego artykułu, w odniesieniu do bezpieczeństwa przetwarzania danych SIS przez organy, o których mowa w art. 44.  4. Środki opisane w ust. 1, 2 i 3 mogą stanowić część ogólnego podejścia i planu w zakresie bezpieczeństwa na szczeblu krajowym obejmującego różne systemy informatyczne. W takich przypadkach wymogi przewidziane w niniejszym artykule i ich stosowanie do SIS muszą zostać wyraźnie wskazane w tym planie, który musi zapewniać ich spełnianie. | **T** | Art. 1 pkt 14  Art. 1 pkt 17 | 14)  art. 27 otrzymuje brzmienie:  „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 i art. 10 ust. 1 rozporządzenia 2018/1862;**  4) umożliwienia organom uprawnionym, wskazanym w art. 3–4, przetwarzania danych SIS poprzez Krajowy System Informatyczny (KSI), w szczególności poprzez 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 i 3 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).  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.”;  17) w art. 34 ust. 1 otrzymuje brzmienie:  „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 jestobowiązany, 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.”; | Niezbędna aktualizacja zasad zapewnienia oceny bezpieczeństwa systemu N.SIS. |
|  | **Art. 11** | Artykuł 11  **Poufność – państwa członkowskie**  1. Każde państwo członkowskie stosuje, zgodnie ze swoim prawem krajowym, swoje przepisy dotyczące tajemnicy zawodowej lub innych równoważnych obowiązków w zakresie poufności do wszystkich osób i podmiotów, od których wymaga się pracy z danymi SIS i informacjami uzupełniającymi. Wymóg ten ma zastosowanie również po zakończeniu pełnienia urzędu przez te osoby lub po ustaniu ich zatrudnienia, lub po zakończeniu działalności tych podmiotów.  2. W przypadku gdy dane państwo członkowskie współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS, ściśle monitoruje ono działania wykonawcy, by zapewnić przestrzeganie wszystkich przepisów niniejszego rozporządzenia, w szczególności dotyczących bezpieczeństwa, poufności i ochrony danych.  3. Zarządzania operacyjnego N.SIS lub kopiami technicznymi nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym. | **N** |  |  | Zasady zapewnienia poufności w zakresie pracy z danymi SIS określają Rozdział 3 i 5 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (nie zmieniły się). |
|  | **Art. 12** | Artykuł 12  **Prowadzenie rejestrów na szczeblu krajowym**  1. Państwa członkowskie zapewniają rejestrowanie w swoich N.SIS każdego dostępu do danych osobowych w CS-SIS oraz wszelkiej wymiany takich danych w ramach CS-SIS – w celu sprawdzania, czy dane wyszukiwanie jest zgodne z prawem, monitorowania zgodności przetwarzania danych z prawem, monitorowania własnej działalności, zapewnienia należytego działania N.SIS oraz integralności i bezpieczeństwa danych. Wymóg ten nie ma zastosowania do zautomatyzowanych procesów, o których mowa w art. 4 ust. 6 lit. a), b) i c).  2. Zapisy w rejestrze wskazują w szczególności historię wpisu, datę i godzinę przetwarzania danych, dane wykorzystane do wyszukiwania, odniesienie do przetwarzanych danych oraz indywidualne i niepowtarzalne identyfikatory użytkownika dotyczące właściwego organu i osoby przetwarzającej dane.  3. Na zasadzie odstępstwa od ust. 2 niniejszego artykułu, jeżeli wyszukiwanie przeprowadza się z wykorzystaniem danych daktyloskopijnych lub wizerunku twarzy zgodnie z art. 43, zapisy w rejestrze zamiast danych rzeczywistych wskazują rodzaj danych wykorzystanych do wyszukiwania. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/71  4. Zapisy w rejestrze są wykorzystywane wyłącznie do celu, o którym mowa w ust. 1, i są usuwane po upływie trzech lat od ich utworzenia. Zapisy w rejestrze obejmujące historię wpisów są usuwane po upływie trzech lat od usunięcia wpisów.  5. Zapisy w rejestrze są przechowywane dłużej niż przez okresy, o których mowa w ust. 4, jeśli są niezbędne do dalszego prowadzenia procedur monitorowania, które już się rozpoczęły.  6. Właściwe organy krajowe odpowiedzialne za sprawdzanie, czy dane wyszukiwanie jest zgodne z prawem, za monitorowanie zgodności przetwarzania danych z prawem i monitorowanie własnej działalności oraz za zapewnianie należytego działania N.SIS oraz integralności i bezpieczeństwa danych muszą mieć, w granicach swoich uprawnień i na swój wniosek, dostęp do rejestrów do celów wykonywania swoich obowiązków.  7. Jeżeli państwa członkowskie przeprowadzają zgodnie z prawem krajowym zautomatyzowane wyszukiwania oparte na skanowaniu tablic rejestracyjnych pojazdów silnikowych, korzystając z systemów automatycznego rozpoznawania tablic rejestracyjnych, państwa członkowskie prowadzą rejestr wyszukiwania zgodnie z prawem krajowym. W razie konieczności można przeprowadzić w SIS pełne wyszukiwanie w celu sprawdzenia, czy uzyskano trafienie. Ust. 1–6 stosuje się do każdego przypadku pełnego wyszukiwania.  8. Komisja przyjmuje akty wykonawcze w celu określenia treści rejestru, o którym mowa w ust. 7 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 2 lit. f  Art. 1 pkt 14 | f) w pkt 19 kropkę zastępuje się średnikiem i dodaje się pkt 20–27 w brzmieniu:  „20) dopasowaniu danych SIS – rozumie się przez to dopasowanie, o którym mowa w art. 3 pkt 7 rozporządzenia 2018/1861 i art. 3 pkt 6 rozporządzenia 2018/1862;  21) tożsamości przywłaszczonej – rozumie się przez to dane wprowadzone do SIS zgodnie z art. 47 rozporządzenia 2018/1861 oraz zgodnie z art. 62 rozporządzenia 2018/1862dotyczące osoby pokrzywdzonej, której tożsamością posługuje się osoba poszukiwana na podstawie wpisu do SIS;  22) odsyłaczu – rozumie się przez to odsyłacz, o którym mowa w art. 48 rozporządzenia 2018/1861 i art. 63 rozporządzenia 2018/1862, utworzony w SIS pomiędzy co najmniej dwoma wpisami;  23) danych biometrycznych – rozumie się przez to dane, o których mowa w art. 3 pkt 13 rozporządzenia 2018/1861 i art. 3 pkt 12 rozporządzenia 2018/1862;  24) danych daktyloskopijnych – rozumie się przez to dane, o których mowa w art. 3 pkt 14 rozporządzenia 2018/1861 i art. 3 pkt 13 rozporządzenia 2018/1862;  **25) użytkowniku indywidualnym - należy przez to rozumieć 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;**  **26) użytkowniku instytucjonalnym - należy przez to rozumieć organ uprawniony do dostępu i współpracy z Krajowym Systemem Informatycznym (KSI) za pośrednictwem własnego systemu teleinformatycznego;**  **27) użytkowniku końcowym - należy przez to rozumieć osobę fizyczną upoważnioną do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI) za pośrednictwem systemu teleinformatycznego użytkownika instytucjonalnego.”;**  14) art. 27 otrzymuje brzmienie:  „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 i art. 10 ust. 1 rozporządzenia 2018/1862;  4) umożliwienia organom uprawnionym, wskazanym w art. 3–4, przetwarzania danych SIS poprzez Krajowy System Informatyczny (KSI), w szczególności poprzez 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 i 3 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).**  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.”; | Wprowadzono nowe kategorie użytkowników KSI, aktualizujące zasady dostępu użytkowników opisane w rozdziale 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym zgodnie z art. 12 rozporządzenia.  Art. 12 ust. 8 nie wymaga transpozycji. |
|  | **Art. 13** | Artykuł 13  **Monitorowanie własnej działalności** Państwa członkowskie zapewniają, aby każdy organ uprawniony do dostępu do danych SIS podejmował niezbędne środki w celu zapewniania przestrzegania niniejszego rozporządzenia oraz w razie potrzeby współpracował z organem nadzorczym. | **T** | Art. 1 pkt 14 | Patrz powyższy punkt |  |
|  | **Art. 14** | Artykuł 14  **Szkolenie personelu**  1. Przed otrzymaniem upoważnienia do przetwarzania danych przechowywanych w SIS i okresowo po przyznaniu dostępu do danych SIS personel organów mających prawo dostępu do SIS przechodzi odpowiednie szkolenie w zakresie bezpieczeństwa danych, praw podstawowych, w tym zasad dotyczących ochrony danych, oraz procedur regulujących przetwarzanie danych określonych w podręczniku SIRENE. Członkowie personelu zostają poinformowani o wszelkich stosownych przepisach dotyczących przestępstw i sankcji, w tym sankcji przewidzianych w art. 73.  2. Państwa członkowskie przyjmują krajowe programy szkoleń w zakresie SIS, które obejmują szkolenia skierowane do użytkowników końcowych oraz do personelu biur SIRENE. Taki program szkoleń może stanowić część ogólnego programu szkoleniowego na szczeblu krajowym, obejmującego szkolenia w innych odpowiednich dziedzinach.  3. W celu zacieśnienia współpracy między biurami SIRENE co najmniej raz w roku organizuje się na szczeblu Unii wspólne kursy szkoleniowe. | **T** | Art. 1 pkt 11 | 11) art. 25 otrzymuje brzmienie:  „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 upoważnia użytkownika indywidualnego do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI), wydaje osobisty i niepowtarzalny identyfikator użytkownika indywidualnego, a także prowadzi ewidencję tych użytkowników.  4. Organ uprawniony, 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.  5. Upoważnienie oraz ewidencja wskazane w ust. 3 i 4 zawierają:  1) imię i nazwisko użytkownika;  2) numer PESEL użytkownika;  3) zakres przyznawanych użytkownikowi uprawnień;  4) okres, na który przyznaje się uprawnienia.  Upoważnienie dla użytkownika końcowego może zawierać dane inne niż wymienione wyłącznie, jeżeli są one niezbędne do nadania uprawnień użytkownikowi końcowemu do systemu teleinformatycznego użytkownika instytucjonalnego.  6. 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 wydawanych do 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.  7. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, tryb dostępu do Krajowego Systemu Informatycznego (KSI) oraz tryb cofania dostępu, sposób przydzielania osobom upoważnionym do dostępu osobistych i niepowtarzalnych identyfikatorów użytkownika indywidualnego, jak również sposób prowadzenia ewidencji użytkowników końcowych oraz użytkowników indywidualnych, a także wzór upoważnienia 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).”; |  |
|  | **Art. 15** | Artykuł 15  **Zarządzanie operacyjne**  1. eu-LISA odpowiada za zarządzanie operacyjne systemem centralnym SIS.eu-LISA – we współpracy z państwami członkowskimi – zapewnia, by w systemie centralnym SIS stosowane były zawsze najlepsze dostępne rozwiązania technologiczne w oparciu o analizę kosztów i korzyści.  2. eu-LISA odpowiada również za następujące zadania związane z infrastrukturą łączności: a) nadzór; b) bezpieczeństwo; c) koordynowanie stosunków między państwami członkowskimi a dostawcą; d) zadania związane z wykonywaniem budżetu; e) zakupy i odnawianie; oraz f) kwestie dotyczące umów. L 312/72 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 3. eu-LISA odpowiada również za następujące zadania związane z biurami SIRENE i łącznością między biurami SIRENE: a) koordynowanie działań w zakresie testowania, zarządzanie tymi działaniami i ich wspieranie; b) utrzymanie i aktualizowanie specyfikacji technicznych dotyczących wymiany informacji uzupełniających między biurami SIRENE a infrastrukturą łączności; oraz c) zarządzanie wpływem zmian technicznych, gdy dotyczy on zarówno SIS, jak i wymiany informacji uzupełniających między biurami SIRENE.  4. eu-LISA opracowuje i utrzymuje mechanizm i procedury na potrzeby przeprowadzania kontroli jakości danych w CS-SIS. Przekazuje ona w tym zakresie regularne sprawozdania państwom członkowskim. eu-LISA przekazuje Komisji regularne sprawozdania, w których uwzględnia napotkane problemy i państwa członkowskie, których problemy te dotyczą. Komisja przekazuje Parlamentowi Europejskiemu i Radzie regularne sprawozdania na temat napotkanych problemów związanych z jakością danych.  5. eu-LISA wykonuje także zadania związane z organizacją szkoleń na temat technicznego użytkowania SIS oraz środków służących poprawie jakości danych SIS.  6. Zarządzanie operacyjne systemem centralnym SIS obejmuje wszystkie zadania niezbędne do zapewnienia funkcjonowania systemu centralnego SIS zgodnie z niniejszym rozporządzeniem przez 24 godziny na dobę, 7 dni w tygodniu – w szczególności prace konserwacyjne oraz udoskonalenia techniczne niezbędne do sprawnego działania systemu. Zadania te obejmują również koordynowanie działań w zakresie testowania, zarządzanie tymi działaniami i ich wspieranie w odniesieniu do systemu centralnego SIS i N.SIS, które zapewniają funkcjonowanie systemu centralnego SIS i N.SIS zgodnie z wymogami zgodności pod względem technicznym i funkcjonalnym określonymi w art. 9.  7. Komisja przyjmuje akty wykonawcze w celu określenia wymogów technicznych dotyczących infrastruktury łączności. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **N** |  |  | Przepis dotyczy Agencji eu-LISA i Komisji Europejskiej. |
|  | **Art. 16** | Artykuł 16  **Bezpieczeństwo – eu-LISA**  1. W odniesieniu do systemu centralnego SIS i infrastruktury łączności eu-LISA przyjmuje niezbędne środki, obejmujące plan bezpieczeństwa, plan ciągłości działania i plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, aby: a) zapewnić fizyczną ochronę danych, w tym poprzez sporządzenie planów awaryjnych służących ochronie infrastruktury krytycznej; b) uniemożliwić osobom nieuprawnionym dostęp do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury); c) zapobiegać nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych); d) zapobiegać nieuprawnionemu wprowadzaniu danych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania); e) zapobiegać korzystaniu z systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników); f) zapobiegać nieuprawnionemu przetwarzaniu danych w SIS oraz nieuprawnionemu zmienianiu lub usuwaniu danych przetwarzanych w SIS (kontrola wprowadzania danych); g) zapewnić, by osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadanym przez nie uprawnieniem, wyłącznie za pomocą indywidualnych i niepowtarzalnych identyfikatorów użytkownika oraz poufnego trybu dostępu (kontrola dostępu do danych); h) stworzyć profile z opisem funkcji i zadań osób, które są uprawnione do dostępu do danych lub do infrastruktury przetwarzania danych, i niezwłocznie udostępniać te profile Europejskiemu Inspektorowi Ochrony Danych na jego wniosek (profile personelu); i) zapewnić możliwość weryfikacji i stwierdzania, którym podmiotom można przesyłać dane osobowe za pośrednictwem sprzętu do przesyłu danych (kontrola przesyłu danych); j) zapewnić możliwość późniejszej weryfikacji i stwierdzania, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania danych oraz kiedy i przez kogo (kontrola wprowadzania danych); 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/73 k) zapobiegać nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas transportu nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania (kontrola transportu); l) monitorować skuteczność środków bezpieczeństwa, o których mowa w niniejszym ustępie, oraz stosować konieczne środki organizacyjne dotyczące monitorowania wewnętrznego, aby zapewnić przestrzeganie niniejszego rozporządzenia (kontrolowanie własnej działalności); m) zapewnić w razie przerwy w działaniu możliwość przywrócenia normalnego funkcjonowania zainstalowanych systemów (odzyskiwanie); n) zapewnić, by SIS wykonywał właściwie swoje funkcje, by błędy były zgłaszane (niezawodność) i by dane osobowe przechowywane w SIS nie mogły ulec uszkodzeniu w wyniku nieprawidłowego funkcjonowania systemu (integralność); oraz o) zapewnić bezpieczeństwo swoich centrów technicznych.  2. eu-LISA stosuje środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do bezpieczeństwa przetwarzania i wymiany informacji uzupełniających przy użyciu infrastruktury łączności. | **N** |  |  | Przepis dotyczy Agencji eu-LISA |
|  | **Art. 17** | Artykuł 17  **Poufność – eu-LISA**  1. Bez uszczerbku dla art. 17 regulaminu pracowniczego, eu-LISA stosuje odpowiednie przepisy dotyczące tajemnicy zawodowej lub innych równoważnych obowiązków w zakresie poufności – o standardzie porównywalnym do tych ustanowionych w art. 11 niniejszego rozporządzenia – do wszystkich swoich pracowników, od których wymaga się pracy z danymi SIS. Wymóg ten ma zastosowanie również po zakończeniu pełnienia urzędu przez te osoby lub po ustaniu ich zatrudnienia, lub po zakończeniu ich działalności.  2. eu-LISA stosuje środki równoważne środkom, o których mowa w ust. 1, w odniesieniu do poufności w zakresie wymiany informacji uzupełniających przy użyciu infrastruktury łączności.  3. W przypadku gdy eu-LISA współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS, monitoruje ona ściśle działania wykonawcy, by zapewnić przestrzeganie wszelkich przepisów niniejszego rozporządzenia, w szczególności przepisów dotyczących bezpieczeństwa, poufności i ochrony danych.  4. Zarządzania operacyjnego CS-SIS nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym | **N** |  |  | Przepis dotyczy Agencji eu-LISA |
|  | **Art. 18** | Artykuł 18  **Prowadzenie rejestrów na szczeblu centralnym**  1. eu-LISA zapewnia rejestrowanie każdego dostępu do danych osobowych w CS-SIS oraz wszelkiej wymiany takich danych w ramach CS-SIS w celach, o których mowa w art. 12 ust. 1. 2. Zapisy w rejestrze wskazują w szczególności historię wpisu, datę i godzinę przetwarzania danych, dane wykorzystane do wyszukiwania, odniesienie do przetwarzanych danych oraz indywidualne i niepowtarzalne identyfikatory użytkownika dotyczące właściwego organu przetwarzającego dane.  3. Na zasadzie odstępstwa od ust. 2 niniejszego artykułu, jeżeli wyszukiwanie przeprowadza się z wykorzystaniem danych daktyloskopijnych lub wizerunków twarzy zgodnie z art. 43, zapisy w rejestrze zamiast danych rzeczywistych wskazują rodzaj danych wykorzystanych do wyszukiwania.  4. Zapisy w rejestrze są wykorzystywane wyłącznie do celów, o których mowa w ust. 1, i są usuwane po upływie trzech lat od ich utworzenia. Zapisy w rejestrze obejmujące historię wpisów są usuwane po upływie trzech lat od usunięcia wpisów.  5. Zapisy w rejestrze mogą być przechowywane dłużej niż przez okresy, o których mowa w ust. 4, jeśli są niezbędne do dalszego prowadzenia procedur monitorowania, które już się rozpoczęły.  6. Do celów monitorowania własnej działalności i zapewnienia należytego działania CS-SIS oraz integralności i bezpieczeństwa danych eu-LISA ma dostęp do rejestrów w granicach swoich uprawnień. Europejski Inspektor Ochrony Danych ma dostęp do tych rejestrów na swój wniosek, w granicach swoich uprawnień i do celów wykonywania swoich zadań. | **N** |  |  | Przepis dotyczy Agencji eu-LISA |
|  | **Art. 19** | Artykuł 19  **Kampanie informacyjne dotyczące SIS**  W momencie rozpoczęcia stosowania niniejszego rozporządzenia Komisja – we współpracy z krajowymi organami nadzorczymi i Europejskim Inspektorem Ochrony Danych – przeprowadza kampanię informacyjną, w ramach której informuje opinię publiczną o celach SIS, danych przechowywanych w SIS, organach mających dostęp do SIS oraz prawach przysługujących osobom, których dane dotyczą. Komisja regularnie powtarza takie kampanie, we współpracy z organami nadzorczymi i Europejskim Inspektorem Ochrony Danych. Komisja prowadzi ogólnodostępną stronę internetową poświęconą wszelkim stosownym informacjom związanym z SIS. Państwa członkowskie – we współpracy ze swoimi organami nadzorczymi – opracowują i wprowadzają w życie niezbędne strategie służące ogólnemu informowaniu obywateli i rezydentów o SIS. | **N** |  |  | Przepis dotyczy działań podejmowanych centralnie przez Komisję Europejska w porozumieniu z krajami członkowskimi |
|  | **Art. 20** | Artykuł 20  **Kategorie danych**  1. Bez uszczerbku dla art. 8 ust. 1 lub dla przepisów niniejszego rozporządzenia dotyczących przechowywania danych dodatkowych, SIS zawiera wyłącznie te kategorie danych dostarczanych przez każde państwo członkowskie, których wymagają cele określone w art. 26, 32, 34, 36, 38 i 40.  2. Kategorie danych są następujące: a) informacje na temat osób, w odniesieniu do których został wprowadzony wpis; b) informacje na temat przedmiotów, o których mowa w art. 26, 32, 34, 36 i 38. 3. Każdy wpis w SIS, który zawiera informacje na temat osób, obejmuje wyłącznie następujące dane: a) nazwiska; b) imiona; c) imiona i nazwiska nadane przy urodzeniu; d) poprzednio używane imiona i nazwiska oraz pseudonimy; e) wszelkie szczególne obiektywne cechy fizyczne niepodlegające zmianom; f) miejsce urodzenia; g) data urodzenia; h) płeć; i) wszelkie posiadane obywatelstwa; j) informacje o tym, czy dana osoba: (i) jest uzbrojona; (ii) jest agresywna; (iii) ukryła się lub uciekła; (iv) wykazuje skłonności samobójcze; (v) stanowi zagrożenie dla zdrowia publicznego; lub (vi) jest zaangażowana w działalność, o której mowa w art. 3–14 dyrektywy (UE) 2017/541; k) podstawa wpisu; l) organ, który utworzył wpis; m) odesłanie do decyzji będącej podstawą wpisu; n) działanie, które należy podjąć w przypadku trafienia; o) odsyłacze do innych wpisów zgodnie z art. 63; p) rodzaj przestępstwa; q) numer rejestracyjny danej osoby w rejestrze krajowym; r) w odniesieniu do wpisów, o których mowa w art. 32 ust. 1 – kategoryzacja rodzaju spraw; s) kategoria dokumentów identyfikacyjnych danej osoby; 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/75 t) państwo wydania dokumentów identyfikacyjnych danej osoby; u) numer lub numery dokumentów identyfikacyjnych danej osoby; v) data wydania dokumentów identyfikacyjnych danej osoby; w) fotografie i wizerunki twarzy; x) zgodnie z art. 42 ust. 3 – odpowiednie profile DNA; y) dane daktyloskopijne; z) kopia, w miarę możliwości w kolorze, dokumentów identyfikacyjnych.  4. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2 i 3 niniejszego artykułu, a także wspólnych norm, o których mowa w ust. 5 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2.  5. Przepisy techniczne są podobne dla wyszukiwań w CS-SIS, w kopiach krajowych lub wspólnych kopiach oraz w kopiach technicznych sporządzanych na podstawie art. 56 ust. 2. Ich podstawę stanowią wspólne normy. | **T** | Art. 1 pkt 2 lit. a | pkt 5 otrzymuje brzmienie:  „5) danych SIS – rozumie się przez 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 7.12.2018, str. 1), zwanego dalej „rozporządzeniem 2018/1860”, w art. 20 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (EU) 2018/1861z 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 7.12.2018, str. 14, z późn. zm.), 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 7.12.2018, str. 56, z późn. zm.), zwanego dalej „rozporządzeniem 2018/1862;”, | Konieczność zaktualizowania definicji w ustawie  Art. 20 ust. 4 nie wymaga transpozycji. |
|  | **Art. 21** | Artykuł 21  **Proporcjonalność**  1. Przed wprowadzeniem wpisu i przy przedłużeniu okresu ważności wpisu państwa członkowskie oceniają, czy dany przypadek jest wystarczająco adekwatny, odpowiedni i ważny, by uzasadnić wpis w SIS. 2. Jeżeli dana osoba lub dany przedmiot są poszukiwane na podstawie wpisu dotyczącego przestępstwa terrorystycznego, dany przypadek uznaje się za wystarczająco adekwatny, odpowiedni i ważny, by uzasadnić wpis w SIS. Ze względu na bezpieczeństwo publiczne lub narodowe państwa członkowskie mogą wyjątkowo nie wprowadzać wpisu, jeśli istnieje prawdopodobieństwo, że utrudniłby on prowadzenie dochodzeń urzędowych lub sądowych, postępowań przygotowawczych lub innych postępowań. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 22** | Artykuł 22  **Wymóg warunkujący wprowadzenie wpisu**  1. Minimalny zestaw danych niezbędnych do wprowadzenia wpisu do SIS obejmuje dane, o których mowa w art. 20 ust. 3 lit. a), g), k) i n), z wyjątkiem sytuacji, o których mowa w art. 40. Inne dane, o których mowa w tym ustępie, także wprowadza się do SIS, jeśli są dostępne.  2. Dane, o których mowa w art. 20 ust. 3 lit. e) niniejszego rozporządzenia, wprowadza się wyłącznie w przypadkach gdy jest to bezwzględnie niezbędne do identyfikacji danej osoby. Jeżeli takie dane zostaną wprowadzone, państwa członkowskie zapewniają przestrzeganie art. 10 dyrektywy (UE) 2016/680. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości  W zakresie art. 22 ust. 2 - ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r., poz. 125) – w tytule ww. ustawy dodano odnośnik nr 1 w brzmieniu: Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89). |
|  | **Art. 23** | Artykuł 23  **Zgodność wpisów**  1. Przed wprowadzeniem wpisu państwo członkowskie sprawdza, czy w SIS istnieje już wpis dotyczący danej osoby lub danego przedmiotu. Aby sprawdzić, czy istnieje już wpis dotyczący danej osoby, przeprowadza się również sprawdzanie przy użyciu danych daktyloskopijnych, jeżeli dane takie są dostępne.  2. Państwo członkowskie wprowadza do SIS tylko jeden wpis dotyczący danej osoby lub danego przedmiotu. W razie potrzeby inne państwa członkowskie mogą wprowadzić nowe wpisy dotyczące tej samej osoby lub tego samego przedmiotu, zgodnie z ust. 3.  3. Jeżeli istnieje już w SIS wpis dotyczący danej osoby lub danego przedmiotu, państwo członkowskie, które chce wprowadzić nowy wpis, sprawdza, czy między wpisami nie ma niezgodności. Jeżeli niezgodności nie ma, państwo członkowskie może wprowadzić nowy wpis. Jeżeli wpisy są ze sobą niezgodne, odpowiednie biura SIRENE państw członkowskich konsultują się ze sobą, dokonując wymiany informacji uzupełniających w celu osiągnięcia porozumienia. Zasady dotyczące zgodności wpisów określa się w podręczniku SIRENE. Po przeprowadzeniu między państwami członkowskimi konsultacji można odstąpić od zasad dotyczących zgodności wpisów z uwagi na istotny interes narodowy.  4. Jeżeli uzyskano trafienia w następstwie wielokrotnych wpisów dotyczących tej samej osoby lub tego samego przedmiotu, wykonujące państwo członkowskie przestrzega zasad dotyczących priorytetu poszczególnych wpisów, które to zasady określono w podręczniku SIRENE. L 312/76 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 Jeżeli danej osoby dotyczą wielokrotne wpisy wprowadzone przez różne państwa członkowskie, w pierwszej kolejności wykonywane są wpisy mające doprowadzić do aresztowania wprowadzone zgodnie z art. 26, z zastrzeżeniem art. 25. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 24** | Artykuł 24  **Przepisy ogólne o umieszczaniu zastrzeżeń**  1. Jeżeli państwo członkowskie uzna, że wykonanie działania wymaganego we wpisie wprowadzonym zgodnie z art. 26, 32 lub 36 jest niezgodne z jego prawem krajowym, jego zobowiązaniami międzynarodowymi lub istotnym interesem narodowym, państwo to może zażądać umieszczenia przy wpisie zastrzeżenia wskazującego, że działanie, które należy podjąć na podstawie wpisu, nie zostanie podjęte na jego terytorium. Zastrzeżenie jest umieszczane przez biuro SIRENE państwa członkowskiego dokonującego wpisu.  2. W celu umożliwienia państwom członkowskim występowania z żądaniem wprowadzenia zastrzeżenia przy wpisie dokonanym zgodnie z art. 26, wszystkie państwa członkowskie są automatycznie informowane – w drodze wymiany informacji uzupełniających – o każdym nowym wpisie tej kategorii. 3. Jeżeli w szczególnie pilnych i poważnych przypadkach państwo członkowskie dokonujące wpisu zażąda wykonania danego działania, wykonujące państwo członkowskie bada, czy jest w stanie zezwolić na usunięcie zastrzeżenia umieszczonego przy wpisie na jego żądanie. Jeżeli wykonujące państwo członkowskie jest w stanie na to zezwolić, podejmuje niezbędne środki w celu zapewnienia, by działanie, które ma zostać podjęte, zostało natychmiast przeprowadzone. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 25** | Artykuł 25  **Zastrzeżenia przy wpisach mających doprowadzić do aresztowania osób w celu ich wydania**  1. Jeżeli zastosowanie ma decyzja ramowa 2002/584/WSiSW, państwo członkowskie zwraca się do państwa członkowskiego dokonującego wpisu o umieszczenie we wpisie mającym doprowadzić do aresztowania osoby w celu jej wydania zastrzeżenia zapobiegającego aresztowaniu w przypadku, gdy organ wymiaru sprawiedliwości właściwy na mocy prawa krajowego w sprawach wykonania europejskiego nakazu aresztowania odmówił wykonania nakazu w oparciu o podstawę do odmowy wykonania i gdy zażądano umieszczenia zastrzeżenia. Państwo członkowskie może również zażądać umieszczenia przy wpisie zastrzeżenia, jeżeli podczas procedury wydawania właściwy organ wymiaru sprawiedliwości tego państwa zwolni osobę, której dotyczy wpis.  2. Niemniej na wniosek organu wymiaru sprawiedliwości właściwego na mocy prawa krajowego, na podstawie ogólnej instrukcji lub w konkretnej sprawie, państwo członkowskie może również zwrócić się do państwa dokonującego wpisu o umieszczenie zastrzeżenia przy wpisie mającym doprowadzić do aresztowania osoby w celu jej wydania, jeżeli jest oczywiste, że konieczna będzie odmowa wykonania europejskiego nakazu aresztowania. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 26** | Artykuł 26  **Cele i warunki dokonywania wpisów**  1. Wpisy dotyczące osób poszukiwanych w celu ich aresztowania i wydania na podstawie europejskiego nakazu aresztowania lub wpisy dotyczące osób poszukiwanych w celu ich aresztowania i ekstradycji są wprowadzane na wniosek organu wymiaru sprawiedliwości państwa członkowskiego dokonującego wpisu. 2. Wpisy mające doprowadzić do aresztowania w celu wydania są również wprowadzane na podstawie nakazów aresztowania wydawanych zgodnie z umowami, które Unia zawarła na podstawie Traktatów z państwami trzecimi w celu wydawania osób na podstawie nakazu aresztowania i które przewidują przekazywanie takiego nakazu aresztowania za pośrednictwem SIS.  3. W przypadku odesłania w niniejszym rozporządzeniu do przepisów decyzji ramowej 2002/584/WSiSW uznaje się, że zastosowanie mają także odpowiednie postanowienia umów, które Unia zawarła na podstawie Traktatów z państwami trzecimi w celu wydawania osób na podstawie nakazu aresztowania i które przewidują przekazywanie takiego nakazu aresztowania za pośrednictwem SIS.  4. W przypadku trwającej operacji państwo członkowskie dokonujące wpisu może tymczasowo uniemożliwić użytkownikom końcowym w państwach członkowskich uczestniczących w danej operacji dostęp do wyszukiwania istniejącego wpisu mającego doprowadzić do aresztowania, wprowadzonego zgodnie z niniejszym artykułem. W takim przypadku dostęp do wpisu mają wyłącznie biura SIRENE. Państwa członkowskie uniemożliwiają dostęp do wyszukiwania wpisu, gdy: a) celu operacji nie można osiągnąć przy zastosowaniu innych środków; b) właściwy organ wymiaru sprawiedliwości państwa członkowskiego dokonującego wpisu udzielił uprzedniej zgody; oraz c) wszystkie państwa członkowskie uczestniczące w operacji zostały poinformowane w drodze wymiany informacji uzupełniających. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/77 Z funkcji przewidzianej w akapicie pierwszym korzysta się wyłącznie przez okres nieprzekraczający 48 godzin. Jeżeli jednak jest to niezbędne z operacyjnego punktu widzenia, okres ten można przedłużyć o kolejne 48-godzinne okresy. Państwa członkowskie prowadzą statystyki dotyczące liczby wpisów, w odniesieniu do których zastosowano tę funkcję.  5. Jeżeli istnieje wyraźna przesłanka wskazująca, że przedmioty, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h), j) i k), są powiązane z osobą, której dotyczy wpis dokonany zgodnie z ust. 1 i 2 niniejszego artykułu, można wprowadzić wpisy dotyczące tych przedmiotów w celu zlokalizowania tej osoby. W takich przypadkach pomiędzy wpisem dotyczącym osoby i wpisem dotyczącym przedmiotu zostaje utworzony odsyłacz zgodnie z art. 63.  6. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów niezbędnych do wprowadzania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 5 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 2 | Art. 3 otrzymuje brzmienie  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 prokuratorowi;  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 przewiduje przekazywanie takiego nakazu aresztowania za pośrednictwem SIS przysługuje sądowi;  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 prokuratora, który wprowadził wpis, może wystąpić Policja, Straż Graniczna lub Agencji Bezpieczeństwa Wewnętrznego. | Konieczność aktualizacji art. 3. wynika z wprowadzenia nowej kategorii podstawy wpisu do SIS w tej kategorii, tj. osób poszukiwanych do zatrzymania  Art. 26 ust. 6 nie wymaga transpozycji. |
|  | **Art. 27** | Artykuł 27  **Dane dodatkowe dotyczące osób poszukiwanych w celu ich aresztowania i wydania**  1. Jeżeli dana osoba jest poszukiwana w celu jej aresztowania i wydania na podstawie europejskiego nakazu aresztowania, państwo członkowskie dokonujące wpisu wprowadza do SIS kopię oryginału europejskiego nakazu aresztowania. Państwo członkowskie może wprowadzić do wpisu mającego doprowadzić do aresztowania osoby w celu jej wydania kopię więcej niż jednego europejskiego nakazu aresztowania.  2. Państwo członkowskie dokonujące wpisu może wprowadzić kopię tłumaczenia europejskiego nakazu aresztowania na co najmniej jeden z języków urzędowych instytucji Unii. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 28** | Artykuł 28  **Informacje uzupełniające o osobach poszukiwanych w celu ich aresztowania i wydania**  Państwo członkowskie wprowadzające wpis mający doprowadzić do aresztowania osoby w celu jej wydania, przekazuje informacje, o których mowa w art. 8 ust. 1 decyzji ramowej 2002/584/WSiSW, pozostałym państwom członkowskim w drodze wymiany informacji uzupełniających. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 29** | Artykuł 29  **Informacje uzupełniające o osobach poszukiwanych w celu ich aresztowania i ekstradycji**  1. Państwo członkowskie wprowadzające wpis do celów ekstradycji, przekazuje pozostałym państwom członkowskim w drodze wymiany informacji uzupełniających następujące dane: a) informację o organie, który wydał wniosek o aresztowanie; b) informację, czy istnieje nakaz aresztowania lub dokument mający taki sam skutek prawny lub wyrok podlegający wykonaniu; c) rodzaj i kwalifikację prawną przestępstwa; d) opis okoliczności, w których przestępstwo zostało popełnione, w tym czas, miejsce oraz formę udziału osoby, w odniesieniu do której wpis został wprowadzony, w popełnieniu przestępstwa; e) w zakresie, w jakim jest to możliwe, informacje o skutkach przestępstwa; oraz f) wszelkie inne informacje przydatne lub niezbędne do tego, by wykonać wpis.  2. Dane wymienione w ust. 1 niniejszego artykułu nie są przekazywane, jeżeli dane, o których mowa w art. 27 lub art. 28, zostały już dostarczone i uznane za wystarczające do wykonania wpisu przez wykonujące państwo członkowskie. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 30** | Artykuł 30  **Przekształcanie działania, które ma zostać podjęte w związku z wpisami dotyczącymi aresztowania w celu wydania lub ekstradycji**  Jeżeli aresztowanie nie może dojść do skutku z uwagi na to, że wezwane do tego państwo członkowskie odmówiło aresztowania zgodnie z procedurami dotyczącymi umieszczania zastrzeżeń określonymi w art. 24 lub 25, lub z uwagi na to, że w przypadku wpisu mającego doprowadzić do aresztowania w celu ekstradycji postępowanie przygotowawcze nie zostało zakończone, państwo członkowskie wezwane do dokonania aresztowania realizuje wpis poprzez podanie informacji o miejscu pobytu danej osoby. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 31** | Artykuł 31  **Wykonanie działania na podstawie wpisu dotyczącego aresztowania w celu wydania lub ekstradycji**  1. Wpis wprowadzony do SIS zgodnie z art. 26 oraz dodatkowe dane, o których mowa w art. 27, stanowią łącznie europejski nakaz aresztowania wydany zgodnie z decyzją ramową 2002/584/WSiSW i mają taki sam skutek jak ten nakaz – w przypadkach, w których ta decyzja ramowa ma zastosowanie.  2. Jeżeli decyzja ramowa 2002/584/WSiSW nie ma zastosowania, wpis wprowadzony do SIS zgodnie z art. 26 i art. 29 ma taki sam skutek prawny jak wniosek o tymczasowe aresztowanie wydany na podstawie art. 16 Europejskiej konwencji o ekstradycji z dnia 13 grudnia 1957 r. lub art. 15 przyjętego w Beneluksie Traktatu o ekstradycji oraz pomocy prawnej w sprawach karnych z dnia 27 czerwca 1962 r. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 32** | Artykuł 32  **Cele i warunki wprowadzania wpisów**  1. Na wniosek właściwego organu państwa członkowskiego dokonującego wpisu, do SIS wprowadzane są wpisy dotyczące następujących kategorii osób: a) osoby zaginione, które muszą zostać objęte ochroną (i) dla ich własnej ochrony; (ii) w celu zapobieżenia zagrożeniu dla porządku publicznego lub bezpieczeństwa publicznego; b) osoby zaginione, które nie muszą zostać objęte ochroną; c) dzieci, które są zagrożone uprowadzeniem przez rodzica, członka rodziny lub opiekuna i którym należy uniemożliwić podróżowanie; d) dzieci, którym należy uniemożliwić podróżowanie ze względu na konkretne i realne zagrożenie, że zostaną wywiezione z terytorium państwa członkowskiego lub opuszczą to terytorium oraz że (i) staną się ofiarami handlu ludźmi lub ofiarami przymusowego małżeństwa, okaleczenia żeńskich narządów płciowych lub innych form przemocy warunkowanej płcią; (ii) staną się ofiarami przestępstw terrorystycznych lub wezmą udział w popełnianiu takich przestępstw; lub (iii) zostaną zwerbowane lub zaciągnięte do ugrupowań zbrojnych lub zmuszone do aktywnego udziału w działaniach wojennych; e) osoby narażone na niebezpieczeństwo, które są pełnoletnie i którym dla ich własnej ochrony należy uniemożliwić podróżowanie, ze względu na konkretne i realne zagrożenie, że zostaną wywiezione z terytorium państwa członkowskiego lub opuszczą to terytorium i że staną się ofiarami handlu ludźmi lub przemocy warunkowanej płcią.  2. Ust. 1 lit. a) ma zastosowanie w szczególności do dzieci i osób, które w następstwie decyzji właściwego organu należy przymusowo umieścić w odpowiedniej placówce.  3. Wpis dotyczący dziecka, o którym mowa w ust. 1 lit. c), wprowadza się w następstwie decyzji właściwych organów, w tym organów wymiaru sprawiedliwości państw członkowskich właściwych w sprawach dotyczących odpowiedzialności rodzicielskiej, jeżeli istnieje konkretne i realne zagrożenie, że dziecko może niezgodnie z prawem zostać wkrótce wywiezione z państwa członkowskiego, w którym znajdują się właściwe organy.  4. Wpis dotyczący osób, o których mowa w ust. 1 lit. d) i e), wprowadza się w następstwie decyzji właściwych organów, w tym organów wymiaru sprawiedliwości.  5. Państwo członkowskie dokonujące wpisu regularnie weryfikuje, czy istnieje potrzeba utrzymywania wpisów, o których mowa w ust. 1 lit. c), d) i e) niniejszego artykułu, zgodnie z art. 53 ust. 4.  6. Państwo członkowskie dokonujące wpisu zapewnia spełnienie następujących wymogów: a) dane, które wprowadza ono do SIS wskazują, do której z kategorii wymienionych w ust. 1 należy osoba, której dotyczy wpis; b) dane, które wprowadza ono do SIS wskazują, o jaki rodzaj sprawy chodzi, o ile rodzaj sprawy jest znany; oraz c) w odniesieniu do wpisów wprowadzanych zgodnie z ust. 1 lit. c), d) i e) wszystkie istotne informacje są dostępne w jego biurze SIRENE od momentu utworzenia wpisu. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/79  7. Cztery miesiące przed tym jak dziecko, którego dotyczy wpis na mocy niniejszego artykułu, osiągnie pełnoletność zgodnie z prawem krajowym państwa członkowskiego dokonującego wpisu, CS-SIS automatycznie powiadamia państwo członkowskie dokonujące wpisu o konieczności aktualizacji podstaw wpisu oraz działania, które ma zostać podjęte, lub o konieczności usunięcia wpisu.  8. Jeżeli istnieje wyraźna przesłanka wskazująca, że przedmioty, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h) i k), są powiązane z osobą, której dotyczy wpis dokonany zgodnie z ust. 1 niniejszego artykułu, można wprowadzić wpisy dotyczące tych przedmiotów w celu zlokalizowania tej osoby. W takich przypadkach pomiędzy wpisem dotyczącym osoby i wpisem dotyczącym przedmiotu zostaje utworzony odsyłacz zgodnie z art. 63.  9. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów dotyczących kategoryzacji rodzajów spraw i wprowadzania danych, o których mowa w ust. 6. Poszczególne rodzaje spraw odnoszących się do osób zaginionych będących dziećmi dotyczą, między innymi, dzieci, które uciekły z domu, dzieci pozbawionych opieki w kontekście migracji oraz dzieci zagrożonych uprowadzeniem przez rodzica. Komisja przyjmuje również akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 8. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 4 | Art. 3 otrzymuje brzmienie  1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS dotyczących:  (...)  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 prokuratorowi;  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 prokuratorowi;  9) małoletnich, którym należy uniemożliwić podróżowanie ze względu na realne zagrożenie, że zostaną wywiezieni z terytorium państwa członkowskiego lub opuszczą to terytorium oraz 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 prokuratorowi;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 i że staną się ofiarami handlu ludźmi lub przemocy warunkowanej płcią przysługuje Policji, Straży Granicznej, sądowi lub prokuratorowi; | **Dodanie art. 3 ust. 1 pkt 7**–**10** ma na celu uwzględnienie nowych zakresów wpisów przetwarzanych w SIS dot. w szczególności małoletnich zagrożonych uprowadzeniem przez rodzica, członka rodziny lub opiekuna oraz małoletnich, którym należy uniemożliwić podróżowanie ze względu na realne zagrożenie, że staną się ofiarami przestępstw o charakterze terrorystycznym lub wezmą udział w popełnianiu takich przestępstw bądź zostaną zwerbowani lub zaciągnięci do ugrupowań zbrojnych lub zmuszeni do aktywnego udziału w działaniach wojennych oraz osób pełnoletnich i małoletnich narażonych na niebezpieczeństwo, którym należy uniemożliwić podróżowanie dla ich własnej ochrony (np. gdy podróż może się wiązać z ryzykiem handlu ludźmi, przymusowego małżeństwa lub przemocą warunkowaną płcią), tzw. „wpisy prewencyjne”.  Przy redakcji art. 3 ust. 1 pkt 7-9 w miejsce użytego w rozporządzeniu 2018/1862 terminu „dziecko” posłużono się pojęciem „małoletni” z uwagi na możliwe trudności w stosowaniu tych przepisów w polskiej praktyce wynikające z braku w polskim prawie jednolitej definicji „dziecka”. Natomiast redagując art. 3 ust. 1 pkt 9 w miejsce użytego w rozporządzeniu 2018/1862 terminu „przestępstwo terrorystyczne” posłużono się pojęciem występującym w polskim systemie prawnym „przestępstwo o charakterze terrorystycznym” (zgodnie z art. 115 § 20 Kodeksu karnego, implementującym decyzję ramową Rady UE 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu; Dz. Urz. UE L 164 z 22.06.2002 r., s. 3.) w celu ujednolicenia pojęć, które dotyczą tego samego zjawiska oraz ze względów gwarancyjnych (prawo karne powinno obejmować ściśle określone czyny zabronione i nie podlegać wykładni rozszerzającej). Ww. terminologię zastosowano także w art. 3 ust. 1 pkt 15.  Art. 32 ust. 9 nie wymaga transpozycji. |
|  | **Art. 33** | Artykuł 33  **Wykonanie działania na podstawie wpisu**  1. W przypadku zlokalizowania osoby, o której mowa w art. 32, właściwe organy wykonującego państwa członkowskiego powiadamiają o miejscu pobytu tej osoby – z zastrzeżeniem wymogów przewidzianych w ust. 4 – państwo członkowskie dokonujące wpisu.  2. W przypadku osób, które należy objąć ochroną zgodnie z art. 32 ust. 1 lit. a), c), d) i e), wykonujące państwo członkowskie natychmiast konsultuje się – w drodze wymiany informacji uzupełniających – ze swoimi właściwymi organami i właściwymi organami państwa członkowskiego dokonującego wpisu w celu niezwłocznego uzgodnienia środków, które należy zastosować. Właściwe organy wykonującego państwa członkowskiego mogą, zgodnie z prawem krajowym, umieścić takie osoby w bezpiecznym miejscu, aby uniemożliwić im kontynuowanie podróży.  3. W sprawach dotyczących dzieci przy podejmowaniu – zgodnie z ust. 2 – decyzji o środkach, które należy zastosować, lub decyzji o umieszczeniu dziecka w bezpiecznym miejscu, należy kierować się najlepszym interesem dziecka. Decyzje takie podejmuje się natychmiast i nie później niż 12 godzin od momentu, gdy dziecko zostało zlokalizowane, po przeprowadzeniu konsultacji z odpowiednimi organami odpowiedzialnymi za ochronę dzieci, stosownie do sytuacji.  4. Dane dotyczące osoby zaginionej, która została zlokalizowana i która jest pełnoletnia, są przekazywane między jednostkami innymi niż właściwe organy wyłącznie za zgodą tej osoby. Właściwe organy mogą jednak przekazać informację o tym, że z powodu zlokalizowania osoby zaginionej wpis został usunięty, osobie, która zgłosiła jej zaginięcie. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 34** | Artykuł 34  **Cele i warunki wprowadzania wpisów**  1. W celu zapewnienia informacji o miejscu zamieszkania lub pobytu osób państwa członkowskie wprowadzają na wniosek właściwego organu wpisy do SIS dotyczące: a) świadków; b) osób wezwanych do stawiennictwa przed organami wymiaru sprawiedliwości w związku z postępowaniem karnym w celu złożenia wyjaśnień w sprawie czynów, za które są ścigane, lub osób poszukiwanych w celu wezwania do takiego stawiennictwa; c) osób, którym ma zostać doręczony wyrok w sprawie karnej lub inne dokumenty związane z postępowaniem karnym, aby złożyły wyjaśnienia w sprawie czynów, za które są ścigane; d) osób, którym ma zostać doręczone wezwanie do stawienia się w celu odbycia kary pozbawienia wolności.  2. Jeżeli istnieje wyraźna przesłanka wskazująca, że przedmioty, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h) i k), są powiązane z osobą, której dotyczy wpis dokonany zgodnie z ust. 1 niniejszego artykułu, można wprowadzić wpisy dotyczące tych przedmiotów w celu zlokalizowania tej osoby. W takich przypadkach pomiędzy wpisami dotyczącymi osoby i wpisem dotyczącym przedmiotu zostaje utworzony odsyłacz zgodnie z art. 63. L 312/80 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018  3. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 4 | Art. 3 otrzymuje brzmienie  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 prokuratorowi;  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 przewiduje przekazywanie takiego nakazu aresztowania za pośrednictwem SIS przysługuje sądowi;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 prokuratorowi; | **Zmiana brzmienia art. 3 ust. 1 pkt 3** jest następstwem dostosowania przepisu do zakresu i warunków wprowadzania wpisów dotyczących czterech kategorii osób poszukiwanych, których obecność jest wymagana do celów postępowania prowadzonego przez organy wymiaru sprawiedliwości, określonych w art. 34 ust. 1 lit. a-d rozporządzenia 2018/1862. W tym zakresie w dotychczasowym stanie prawnym istniała możliwość wpisu jako osoby poszukiwanej dla ustalenia miejsca jej pobytu w przypadku skazanych, wobec których powinien zostać wykonany wyrok w sprawie karnej lub w sprawie o przestępstwo skarbowe lub skazanych wezwanych do stawienia się w celu odbycia kary pozbawienia wolności – natomiast z uwagi na treść art. 34 ust. 1 lit. c-d rozporządzenia UE projekt przewiduje tę możliwość w przypadku osób, którym ma zostać doręczony wyrok w sprawie karnej lub inne dokumenty związane z postępowaniem karnym, aby złożyły wyjaśnienia w sprawie czynów, za które są ścigane oraz osób, którym ma zostać doręczone wezwanie do stawienia się w celu odbycia kary pozbawienia wolności. W projektowanym przepisie, poza odniesieniem do pojęcia „postępowanie karne” - zachowano przy tym wyraźne odniesienie do pojęcia „postępowanie karne skarbowe” – analogicznie do rozwiązania przyjętego w obowiązującym stanie prawnym. Literalne wskazanie drugiej z wymienionych kategorii postępowań uwzględnia specyfikę krajowego porządku prawnego, w którym postępowanie karne skarbowe jest systemowo wyodrębnione. Ma to na celu – jak wskazywano już w dacie nowelizowania ustawy w 2009 r. - uniknięcie wątpliwości interpretacyjnych co do zakresu pojęcia „postępowanie karne”, którym posłużono się redagując ww. przepis rozporządzenia UE, na rzecz ujęcia „spraw karnych skarbowych” w zakresie dyspozycji tego przepisu. Ww. redakcję zastosowano konsekwentnie do całości projektu. Dodatkowo, przy redakcji tego przepisu dostosowano w miarę możliwości kategorie osób, określonych opisowo w przepisach rozporządzenia, do terminologii użytej w przepisach Kodeksu postępowania karnego dla zapewnienia spójności regulacji w polskim porządku prawnym. Nadto, poszczególne kategorie osób wymienione zostały z zastosowanie spójnika alternatywy rozłącznej, by wykluczyć ewentualne wątpliwości interpretacyjne co do rozdzielnego traktowania określonych fragmentów tego przepisu w kontekście regulacji unijnej (w rozporządzeniu kategorie te wskazane są oddzielnie) oraz w kontekście przypisanego poszukiwaniu tych osób celu – tj. zapewnienia informacji o miejscu zamieszkania lub pobytu (a więc nie tylko sytuacji, w której miejsce to pozostaje nieznane) niezależnie każdej z wymienionych kategorii osób.  Art. 34 ust. 3 nie wymaga transpozycji. |
|  | **Art. 35** | Artykuł 35  **Wykonanie działania na podstawie wpisu**  Żądane informacje są przekazywane w drodze wymiany informacji uzupełniających państwu członkowskiemu dokonującemu wpisu. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 36** | Artykuł 36  **Cele i warunki wprowadzania wpisów**  1. Wpisy dotyczące osób, przedmiotów, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h), i), k) oraz l), i bezgotówkowych środków płatniczych są wprowadzane zgodnie z prawem krajowym państwa członkowskiego dokonującego wpisu, do celów kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych zgodnie z art. 37 ust. 3, 4 i 5.  2. W przypadku wprowadzania wpisów w celu przeprowadzenia kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych i jeżeli informacje poszukiwane przez państwo członkowskie dokonujące wpisu są informacjami dodatkowymi w stosunku do informacji przewidzianych w art. 37 ust. 1 lit. a)–h), państwo członkowskie dokonujące wpisu umieszcza we wpisie wszystkie informacje, których poszukuje. Jeżeli informacje te dotyczą szczególnych kategorii danych osobowych, o których mowa w art. 10 dyrektywy (UE) 2016/680, są one poszukiwane wyłącznie wtedy, gdy jest to ściśle niezbędne do konkretnego celu wpisu oraz w związku z przestępstwem, w odniesieniu do którego wpis został wprowadzony.  3. Wpisy dotyczące osób w celu przeprowadzania kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych może zostać wprowadzony w celu zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania, w celu wykonania wyroku w sprawach karnych oraz w celu zapobiegania zagrożeniom dla bezpieczeństwa publicznego, jeżeli zachodzi co najmniej jedna z następujących okoliczności: a) jeżeli istnieje wyraźna przesłanka, że dana osoba ma zamiar popełnić lub popełnia którekolwiek z przestępstw, o których mowa w art. 2 ust. 1 i 2 decyzji ramowej 2002/584/WSiSW; b) jeżeli informacje, o których mowa w art. 37 ust. 1, są niezbędne do wykonania kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w odniesieniu do osoby skazanej za popełnienie któregokolwiek z przestępstw, o których mowa w art. 2 ust. 1 i 2 decyzji ramowej 2002/584/WSiSW; c) jeżeli ogólna ocena danej osoby, w szczególności w świetle wcześniej popełnionych przestępstw, pozwala przypuszczać, że osoba ta może w przyszłości popełniać przestępstwa, o których mowa w art. 2 ust. 1 i art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW. 4. Ponadto wpisy dotyczące osób w celu przeprowadzania kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych może zostać wprowadzony zgodnie z prawem krajowym na wniosek organów odpowiedzialnych za bezpieczeństwo narodowe, jeżeli istnieje konkretna przesłanka wskazująca, że informacje, o których mowa w art. 37 ust. 1, są niezbędne do zapobieżenia poważnemu zagrożeniu stwarzanemu przez daną osobę lub innym poważnym zagrożeniom dla wewnętrznego lub zewnętrznego bezpieczeństwa narodowego. Państwo członkowskie, które wprowadziło wpis zgodnie z niniejszym ustępem powiadamia o tym wpisie pozostałe państwa członkowskie. Każde państwo członkowskie określa, którym organom należy przekazywać takie informacje. Informacje są przekazywane za pośrednictwem biur SIRENE.  5. Jeżeli istnieje wyraźna przesłanka wskazująca, że przedmioty, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h), j), k) oraz l), lub bezgotówkowe środki płatnicze są związane z poważnymi przestępstwami, o których mowa w ust. 3 niniejszego artykułu, lub z poważnymi zagrożeniami, o których mowa w ust. 4 niniejszego artykułu, można wprowadzić wpisy dotyczące tych przedmiotów i utworzyć odsyłacz do wpisów wprowadzonych zgodnie z ust. 3 i 4 niniejszego artykułu.  6. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 5 niniejszego artykułu, a także informacji dodatkowych, o których mowa w ust. 2 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 4 | Art. 3 otrzymuje brzmienie  1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS dotyczących:  (…)  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 2021 r. poz. 534 i 1023),  - 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 któregokolwiek 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 popełniać przestępstwa, o których 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;  W zakresie art. 36 ust. 2 - ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r., poz. 125) – w tytule ww. ustawy dodano odnośnik nr 1 w brzmieniu: Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89). | Zmiany w art. 3 ust. 1 pkt 11 lit. a mają na celu dodanie nowego zakresu wpisów przetwarzanych w SIS, tj. wpisów na potrzeby rozpytania kontrolnego, będącego krokiem pośrednim między kontrolą niejawną a kontrolą szczególną, pozwalającym na przesłuchanie danej osoby oraz doprecyzowanie przepisów zgodnie z art. 36 rozporządzenia 2018/1862  Art. 36 ust. 6 nie wymaga transpozycji. |
|  | **Art. 37** | Artykuł 37  **Wykonanie działania na podstawie wpisu**  1. Do celów kontroli niejawnych, rozpytań kontrolnych lub kontroli szczególnych, wykonujące państwo członkowskie gromadzi i przekazuje państwu członkowskiemu dokonującemu wpisu wszystkie lub niektóre z poniższych informacji: a) fakt zlokalizowania osoby, której dotyczy wpis, albo przedmiotów, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h), j), k) oraz l), lub bezgotówkowych środków płatniczych, w odniesieniu do których dokonano wpisu; b) miejsce, godzina i podstawy kontroli; c) trasa i cel podróży; d) osoby towarzyszące osobie, której dotyczy wpis, lub osoby przewożone pojazdem, jednostką pływającą lub statkiem powietrznym lub osoby towarzyszące osobie posiadającej blankiet dokumentu urzędowego lub wydany dokument tożsamości, co do których można w uzasadniony sposób przypuszczać, że pozostają one w związku z osobą, której dotyczy wpis; e) ujawniona tożsamość i opis osoby korzystającej z blankietu dokumentu urzędowego lub wydanego dokumentu tożsamości, których dotyczy wpis; f) przedmioty, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h), j), k) oraz l), lub wykorzystywane bezgotówkowe środki płatnicze; g) przewożone przedmioty, w tym dokumenty podróży; h) okoliczności zlokalizowania osoby lub przedmiotów, o których mowa w art. 38 ust. 2 lit. a), b), c), e), g), h), j), k) oraz l), lub bezgotówkowych środków płatniczych; i) wszelkie inne informacje poszukiwane zgodnie z art. 36 ust. 2 przez państwo członkowskie dokonujące wpisu. Jeżeli informacje, o których mowa w akapicie pierwszym lit. i) niniejszego ustępu, dotyczą szczególnych kategorii danych osobowych, o których mowa w art. 10 dyrektywy (UE) 2016/680, są one przetwarzane zgodnie z warunkami określonymi w tym artykule i wyłącznie wtedy, gdy stanowią uzupełnienie innych danych osobowych przetwarzanych w tym samym celu.  2. Wykonujące państwo członkowskie przekazuje informacje, o których mowa w ust. 1 w drodze wymiany informacji uzupełniających.  3. Kontrola niejawna obejmuje niejawne gromadzenie jak największej liczby informacji, o których mowa w ust. 1, podczas przeprowadzania rutynowych czynności przez właściwe organy krajowe państwa wykonującego. Gromadzenie tych informacji pozostaje bez wpływu na niejawny charakter kontroli, a osoby, której dotyczy wpis, w żadnym przypadku nie można powiadomić o istnieniu wpisu.  4. Rozpytanie kontrolne obejmuje rozpytanie danej osoby, w tym na podstawie informacji lub szczegółowych pytań zamieszczonych we wpisie zgodnie z art. 36 ust. 2 przez państwo członkowskie dokonujące wpisu. Rozpytanie przeprowadza się zgodnie z prawem krajowym wykonującego państwa członkowskiego.  5. Podczas kontroli szczególnych osoby, pojazdy, jednostki pływające, statki powietrzne, kontenery oraz przewożone przedmioty mogą zostać przeszukane w celach, o których mowa w art. 36. Przeszukanie przeprowadza się zgodnie z prawem krajowym państwa wykonującego.  6. Jeżeli kontrole szczególne nie są dopuszczalne w świetle prawa krajowego państwa wykonującego, są one zastępowane w danym państwie członkowskim rozpytaniami kontrolnymi. Jeżeli rozpytania kontrolne nie są dopuszczalne w świetle prawa krajowego państwa wykonującego, są one zastępowane w danym państwie członkowskim kontrolami niejawnymi. Jeżeli zastosowanie ma dyrektywa 2013/48/UE, państwa członkowskie zapewniają, by przestrzegane było prawo osób podejrzanych i oskarżonych do dostępu do adwokata na warunkach określonych w tej dyrektywie.  7. Ust. 6 pozostaje bez uszczerbku dla spoczywającego na państwach członkowskich obowiązku udostępniania użytkownikom końcowym informacji poszukiwanych na mocy art. 36 ust. 2. | **T** | Art. 1 pkt 4 | jak wyżej  W zakresie art. 37 ust. 1 - ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) – w tytule ww. ustawy dodano odnośnik nr 1 w brzmieniu: Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89). | Zapewnienie zgodności działań na podstawie wpisu musi być zgodny z informacjami, o których mowa w art. 37 ust. 1 rozporządzenia 1862/2018 tj. informacje są niezbędne do wykonania kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w odniesieniu do osoby skazanej za popełnienie któregokolwiek z przestępstw, o których mowa w art. 607w KPK |
|  | **Art. 38** | Artykuł 38  **Cele i warunki wprowadzania wpisów**  1. Państwa członkowskie wprowadzają do SIS wpisy dotyczące przedmiotów poszukiwanych w celu ich zajęcia lub w celu ich wykorzystania jako dowód w postępowaniu karnym. L 312/82 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018  2. Wpisy wprowadza się w następujących kategoriach łatwych do zidentyfikowania przedmiotów: 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 ust. 3. W odniesieniu do dokumentów, o których mowa w lit. k), l) i m), państwo członkowskie dokonujące wpisu może wskazać, czy dokumenty takie zostały skradzione, przywłaszczone, utracone, unieważnione lub czy są fałszywe.  3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 75 w celu zmiany niniejszego rozporządzenia poprzez zdefiniowanie nowych podkategorii przedmiotów wymienionych w ust. 2 lit. o), p), q) i r) niniejszego artykułu.  4. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania, aktualizowania, usuwania i wyszukiwania danych, o których mowa w ust. 2 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 4 | Art. 3 otrzymuje brzmienie  1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS dotyczących:  (…)  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 prokuratorowi; | Zmiany w art. 3 ust. 1 pkt 12 mają na celu dodanie nowych kategorii wpisów oraz ujednolicenie listy przedmiotów, zgodnie z art. 38 ust. 2 rozporządzenia 2018/1862  Art. 38 ust. 3 i 4 nie wymagają transpozycji. |
|  | **Art. 39** | Artykuł 39  **Wykonanie działania na podstawie wpisu**  1. Jeżeli wyszukiwanie wykaże istnienie wpisu dotyczącego przedmiotu, który został zlokalizowany, właściwy organ zajmuje ten przedmiot zgodnie ze swoim prawem krajowym i kontaktuje się z organem państwa członkowskiego dokonującego wpisu, tak aby ustalić środki, które należy zastosować. W tym celu dopuszcza się także przekazywanie danych osobowych zgodnie z niniejszym rozporządzeniem.  2. Informacje, o których mowa w ust. 1, są przekazywane w drodze wymiany informacji uzupełniających.  3. Wykonujące państwo członkowskie stosuje środki, o które wniesiono, zgodnie z prawem krajowym. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości |
|  | **Art. 40** | Artykuł 40  **Wpisy dotyczące nieznanych osób poszukiwanych do celów identyfikacji zgodnie z prawem krajowym**  Państwa członkowskie mogą wprowadzić do SIS wpisy dotyczące nieznanych osób, które są poszukiwane, zawierające jedynie dane daktyloskopijne. Takie dane daktyloskopijne stanowią kompletne lub niekompletne zestawy – znalezionych na miejscu popełnienia przestępstw terrorystycznych lub innych poważnych przestępstw będących przedmiotem postępowania przygotowawczego – odbitek linii papilarnych palców lub odbitek linii papilarnych dłoni. Wprowadza się je do SIS wyłącznie wtedy, gdy z bardzo dużym prawdopodobieństwem można stwierdzić, że należą do sprawcy danego przestępstwa. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/83 Jeżeli właściwy organ państwa członkowskiego dokonującego wpisu nie może ustalić tożsamości osoby podejrzanej przy użyciu innej stosownej krajowej, unijnej lub międzynarodowej bazy danych, dane daktyloskopijne, o których mowa w akapicie pierwszym, mogą być wprowadzane w tej kategorii wpisów wyłącznie do zbioru „nieznana osoba poszukiwana” do celów identyfikacji tej osoby. | **T** | Art. 1 pkt 4 | Art. 3 otrzymuje brzmienie  1. Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS dotyczących:  (…)  15) danych daktyloskopijnych znalezionych na miejscu popełnienia przestępstw o charakterze terrorystycznym lub innych poważnych przestępstw będących przedmiotem postępowania przygotowawczego, jeżeli zachodzi wysokie prawdopodobieństwo, że należą do sprawcy, przysługuje Agencji Bezpieczeństwa Wewnętrznego, Policji, Służbie Celno-Skarbowej, Żandarmerii Wojskowej lub Straży Granicznej. | Zmiany w art. 3 ust. 1 pkt 15 mają na celu uzgodnienie listy podmiotów mogących wprowadzać wpisy zgodne z art. 40 Rozporządzenia z art. 312 pkt 1 KPK, zgodnie z którym uprawnienia Policji w zakresie postępowania przygotowawczego przysługują także organom Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Krajowej Administracji Skarbowej, Centralnego Biura Antykorupcyjnego oraz Żandarmerii Wojskowej w zakresie ich właściwości |
|  | **Art. 41** | Artykuł 41  **Wykonanie działania na podstawie wpisu**  W przypadku trafienia dotyczącego danych wprowadzonych zgodnie z art. 40 tożsamość osoby ustala się zgodnie z prawem krajowym, weryfikując z pomocą eksperta, czy dane daktyloskopijne w SIS należą do danej osoby. Wykonujące państwa członkowskie przekazują państwu członkowskiemu dokonującemu wpisu informacje o tożsamości i miejscu pobytu danej osoby w drodze wymiany informacji uzupełniających, tak aby ułatwić odpowiednio szybkie przeprowadzenie postępowania przygotowawczego w danej sprawie. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy jednolitych zasad wprowadzania wpisów nieznanych osób zawierających jedynie dane daktyloskopijne |
|  | **Art. 42** | Artykuł 42  **Przepisy szczegółowe dotyczące wprowadzania fotografii, wizerunków twarzy, danych daktyloskopijnych i profili DNA**  1. Do SIS wprowadzane są wyłącznie fotografie, wizerunki twarzy, dane daktyloskopijne, o których mowa w art. 20 ust. 3 lit. w) i y), które spełniają minimalne normy i specyfikacje techniczne dotyczące jakości danych. Przed wprowadzeniem takich danych przeprowadza się kontrolę jakości w celu ustalenia, czy spełniają one minimalne normy i specyfikacje techniczne dotyczące jakości danych.  2. Dane daktyloskopijne wprowadzane do SIS mogą składać się z jednej do dziesięciu płaskich odbitek linii papilarnych palców i jednej do dziesięciu przetoczonych odbitek linii papilarnych palców. Mogą one również zawierać do dwóch odbitek linii papilarnych dłoni.  3. Profil DNA można dodać do wpisów wyłącznie w sytuacjach przewidzianych w art. 32 ust. 1 lit. a), wyłącznie po przeprowadzeniu kontroli jakości w celu ustalenia, czy spełnione są minimalne normy i specyfikacje techniczne dotyczące jakości danych, oraz wyłącznie w przypadku, gdy fotografie, wizerunki twarzy lub dane daktyloskopijne nie są dostępne lub nie umożliwiają identyfikacji. Profile DNA osób będących bezpośrednimi wstępnymi lub zstępnymi lub rodzeństwem osoby, której dotyczy wpis, mogą zostać dodane do wpisu, pod warunkiem że osoby te udzielą wyraźnej zgody. W przypadku gdy do wpisu dodany zostaje profil DNA, zawiera on minimalne informacje ściśle niezbędne do celów identyfikacji zaginionej osoby.  4. Ustanawia się minimalne normy i specyfikacje techniczne dotyczące jakości danych zgodnie z ust. 5 niniejszego artykułu w odniesieniu do przechowywania danych biometrycznych, o których mowa w ust. 1 i 3 niniejszego artykułu. Te minimalne normy i specyfikacje techniczne dotyczące jakości danych określają poziom jakości wymagany do wykorzystywania danych w celu weryfikacji tożsamości osoby zgodnie z art. 43 ust. 1 i do wykorzystywania danych w celu zidentyfikowania osoby zgodnie z art. 43 ust. 2–4. 5. Komisja przyjmuje akty wykonawcze w celu określenia minimalnych norm i specyfikacji technicznych dotyczących jakości danych, o których mowa w ust. 1, 3 i 4 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 5 | Art. 4 otrzymuje brzmienie  (…)  9. Uprawnienie do weryfikacji dopasowań uzyskanych przez uprawniony organ, opierających się na porównaniu danych biometrycznych przysługuje Centralnemu Laboratorium Kryminalistycznemu Policji.  10. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób i tryb przetwarzania danych biometrycznych SIS oraz wzory dokumentów wykorzystywanych przy przetwarzaniu tych danych, a także sposób i tryb weryfikacji dopasowań opartych na porównaniu danych biometrycznych, uwzględniając procedurę postępowania i warunki techniczne przy pobieraniu, rejestrowaniu i przekazywaniu tych danych.”; | 1. **Art. 1 pkt 5 ustawy nowelizującej – zmiana art. 4**   Z uwagi na dużą ilość zmian w art. 4 ustawy, przedmiotowym przepisom nadane zostało nowe brzmienie. Przy redakcji art. 4 ust. 1 - co do zasady - zastosowano odesłanie do art. 3 ust. 1 celem zachowania przejrzystości jego treści oraz uniknięcia ewentualnych pomyłek.  Art. 42 ust. 4 nie wymaga transpozycji. |
|  | **Art. 43** | Artykuł 43  **Przepisy szczegółowe dotyczące weryfikacji lub wyszukiwania przy użyciu fotografii, wizerunków twarzy, danych daktyloskopijnych i profili DNA**  1. Jeżeli fotografie, wizerunki twarzy, dane daktyloskopijne i profile DNA są dostępne we wpisie w SIS, takie fotografie, wizerunki twarzy, dane daktyloskopijne i profile DNA wykorzystuje się w celu potwierdzenia tożsamości osoby, która została zlokalizowana w wyniku wyszukiwania alfanumerycznego przeprowadzonego w SIS.  2. Wyszukiwanie przy użyciu danych daktyloskopijnych może być przeprowadzone we wszystkich przypadkach w celu identyfikacji danej osoby. Jeżeli jednak tożsamości danej osoby nie można ustalić w żaden inny sposób, w celu identyfikacji przeprowadza się wyszukiwanie przy użyciu danych daktyloskopijnych. W tym celu centralny SIS posiada Automatyczny System Identyfikacji Daktyloskopijnej.  3. Dane daktyloskopijne w SIS związane z wpisami wprowadzonymi zgodnie z art. 26, 32, 36 i 40 można wyszukiwać również przy użyciu kompletnych lub niekompletnych zestawów odbitek linii papilarnych palców lub odbitek linii papilarnych dłoni, które znaleziono na miejscu popełnienia poważnych przestępstw lub przestępstw terrorystycznych będących przedmiotem postępowania przygotowawczego i w przypadku których z dużym prawdopodobieństwem można stwierdzić, że te zestawy odbitek linii papilarnych należą do sprawcy danego przestępstwa i pod warunkiem że wyszukiwanie przeprowadzane jest równolegle w odpowiednich bazach danych państwa członkowskiego zawierających odbitki linii papilarnych palców. L 312/84 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 4. Gdy tylko stanie się to technicznie możliwe oraz przy jednoczesnym zapewnieniu wysokiego stopnia wiarygodności identyfikacji, można będzie wykorzystywać fotografie i wizerunki twarzy do identyfikacji danej osoby na stałych przejściach granicznych. Zanim funkcja ta zostanie wdrożona w SIS, Komisja przedstawi sprawozdanie dotyczące dostępności, gotowości i niezawodności wymaganych rozwiązań technologicznych. Sprawozdanie to zostanie skonsultowane z Parlamentem Europejskim. Po tym, jak funkcja ta zacznie być wykorzystywana na stałych przejściach granicznych, Komisja będzie uprawniona do przyjęcia aktów delegowanych zgodnie z art. 75 w celu uzupełnienia niniejszego rozporządzenia w zakresie określenia innych warunków, w których fotografie i wizerunki twarzy mogą być wykorzystywane do identyfikacji osób. | **T** | Art. 1 pkt 5 | Art. 4 otrzymuje brzmienie  (…)  9. Uprawnienie do weryfikacji dopasowań uzyskanych przez uprawniony organ, opierających się na porównaniu danych biometrycznych przysługuje Centralnemu Laboratorium Kryminalistycznemu Policji.  10. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób i tryb przetwarzania danych biometrycznych SIS oraz wzory dokumentów wykorzystywanych przy przetwarzaniu tych danych, a także sposób i tryb weryfikacji dopasowań opartych na porównaniu danych biometrycznych, uwzględniając procedurę postępowania i warunki techniczne przy pobieraniu, rejestrowaniu i przekazywaniu tych danych.”; | Art. 43 ust. 4 nie wymaga transpozycji. |
|  | **Art. 44** | Artykuł 44  **Właściwe organy krajowe mające prawo do dostępu do danych w SIS**  1. Właściwe organy krajowe mają dostęp do danych wprowadzonych do SIS oraz prawo do wyszukiwania takich danych bezpośrednio lub w kopii bazy danych SIS do celów: a) kontroli granicznej, zgodnie z rozporządzeniem (UE) 2016/399; b) kontroli policyjnych i celnych przeprowadzanych na terytorium danego państwa członkowskiego oraz koordynowania takich kontroli przez wyznaczone organy; c) zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar w danym państwie członkowskim, o ile zastosowanie ma dyrektywa (UE) 2016/680; d) badania warunków i podejmowania decyzji dotyczących wjazdu i pobytu obywateli państw trzecich na terytorium państw członkowskich, w tym dokumentów pobytowych i wiz długoterminowych, oraz dotyczących powrotu obywateli państw trzecich, jak również przeprowadzania kontroli obywateli państw trzecich, którzy nielegalnie wjeżdżają lub przebywają na terytorium państw członkowskich; e) kontroli bezpieczeństwa w odniesieniu do obywateli państw trzecich, którzy ubiegają się o ochronę międzynarodową, o ile organy przeprowadzajace kontrole nie są „organami rozstrzygającymi” zdefiniowanymi w art. 2 lit. f) dyrektywy Parlamentu Europejskiego i Rady 2013/32/UE ( 1 ), oraz w stosownych przypadkach do celów wydawania opinii zgodnie z rozporządzeniem Rady nr (WE) 377/2004 ( 2 ).  2. Prawo do dostępu do danych w SIS oraz prawo do bezpośredniego wyszukiwania takich danych może być wykonywane przez właściwe organy krajowe odpowiedzialne za naturalizację, określone w prawie krajowym, do celów rozpatrywania wniosków o naturalizację.  3. Prawo do dostępu do danych wprowadzonych do SIS oraz prawo do bezpośredniego wyszukiwania takich danych może być wykonywane również przez krajowe organy wymiaru sprawiedliwości, w tym organy odpowiedzialne za wszczynanie postępowań karnych z oskarżenia publicznego i prowadzenie postępowań przygotowawczych przed wniesieniem aktu oskarżenia, w ramach wykonywania ich zadań określonych w prawie krajowym, a także przez organy koordynujące ich działania.  4. Właściwe organy, o których mowa w niniejszym artykule, są uwzględniane w wykazie, o którym mowa w art. 56 ust. 7. | **T** | Art. 1 pkt 4 | art. 3 otrzymuje brzmienie:  „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 prokuratorowi;  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 przewiduje przekazywanie takiego nakazu aresztowania za pośrednictwem SIS przysługuje sądowi;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 prokuratorowi;  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, w tym wymagających ochrony, 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, przysługuje Policji7) 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 prokuratorowi;  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 prokuratorowi;  9) małoletnich, którym należy uniemożliwić podróżowanie ze względu na realne zagrożenie, że zostaną wywiezieni z terytorium państwa członkowskiego lub opuszczą to terytorium oraz 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 prokuratorowi;  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 i że staną się ofiarami handlu ludźmi lub przemocy warunkowanej płcią przysługuje Policji, Straży Granicznej, sądowi lub prokuratorowi11) 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 2021 r. poz. 534 i 1023),  - 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 któregokolwiek 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 popełniać przestępstwa, o których 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 prokuratorowi;  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 wysokie prawdopodobieństwo, że należą do sprawcy, przysługuje Agencji Bezpieczeństwa Wewnętrznego, Policji, Służbie Celno-Skarbowej, Żandarmerii Wojskowej lub Straży Granicznej.  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 ust. 7, art. 40 i art. 44 rozporządzenia 2018/1861 oraz art. 53 ust. 1-7 i ust 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 q i 2, do sądu lub prokuratora, który wprowadził wpis, może wystąpić Policja, Straż Graniczna lub Agencji Bezpieczeństwa Wewnętrznego.  5.  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 SIS określonego w art. 3 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 SIS określonego w art. 3 ust. 1 pkt 1-4 i pkt 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.  W zakresie art. 44 ust. 1 lit. c - ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r., poz. 125) – w tytule ww. ustawy dodano odnośnik nr 1 w brzmieniu: Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89). | modyfikacja listy właściwych organów krajowych mających prawo dostępu do SIS |
|  | **Art. 45** | Artykuł 45  **Służby rejestrujące pojazdy**  1. Służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych pojazdów, o których mowa w dyrektywie Rady 1999/37/WE ( 3 ), mają dostęp do danych wprowadzonych do SIS zgodnie z art. 38 ust. 2 lit. a), b), c), m) i p) niniejszego rozporządzenia wyłącznie w celu sprawdzenia, czy pojazdy oraz towarzyszące im dowody rejestracyjne i tablice rejestracyjne, o których rejestrację zwrócono się do tych służb, zostały skradzione, przywłaszczone, utracone, mają charakter takich dokumentów, ale są fałszywe, lub są poszukiwane jako dowód w postępowaniu karnym. Dostęp służb, o których mowa w akapicie pierwszym, do danych regulowany jest prawem krajowym i jest ograniczony do kompetencji szczególnej danych służb. 2. Służby, o których mowa w ust. 1, będące służbami państwowymi, mają prawo do bezpośredniego dostępu do danych w SIS. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/85 ( 1 ) Dyrektywa Parlamentu Europejskiego i Rady 2013/32/UE z dnia 26 czerwca 2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej (Dz.U. L 180 z 29.6.2013, s. 60). ( 2 ) Rozporządzenie Rady (WE) 377/2004 z dnia 19 lutego 2004 r. w sprawie utworzenia sieci oficerów łącznikowych ds. imigracji (Dz.U. L 64 z 2.3.2004, s. 1). ( 3 ) Dyrektywa Rady 1999/37/WE z dnia 29 kwietnia 1999 r. w sprawie dokumentów rejestracyjnych pojazdów (Dz.U. L 138 z 1.6.1999, s. 57).  3. Służby, o których mowa w ust. 1 niniejszego artykułu, niebędące służbami państwowymi, mają dostęp do danych w SIS wyłącznie za pośrednictwem organu, o którym mowa w art. 44. Organ ten ma prawo do bezpośredniego dostępu do danych i przekazywania ich odpowiednim służbom. Dane państwo członkowskie zapewnia, by przedmiotowe służby i ich pracownicy byli zobowiązani do przestrzegania wszelkich ograniczeń dotyczących dozwolonego wykorzystywania danych przekazywanych im przez ten organ.  4. Art. 39 nie ma zastosowania do dostępu do SIS uzyskanego zgodnie z niniejszym artykułem. Przekazywanie policji lub organom wymiaru sprawiedliwości przez służby, o których mowa w ust. 1 niniejszego artykułu, informacji uzyskanych w wyniku dostępu do SIS regulowane jest prawem krajowym. | **T** | Art. 1 pkt 5 | art. 4 otrzymuje brzmienie  (…)  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 samorządowym właściwym w sprawach rejestracji pojazdów**.  3. Uprawnienie do bezpośredniego 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. h oraz i, przysługuje Prezesowi Urzędu Lotnictwa Cywilnego.  4. 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, staroście lub właściwemu polskiemu związkowi sportowemu w rozumieniu ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133).  5. 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 74 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2021 r. poz. 450, 463, 694 i 720) 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; |  |
|  | **Art. 46** | Artykuł 46  **Służby rejestrujące jednostki pływające i statki powietrzne**  1. Służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych lub za zapewnianie zarządzania ruchem w odniesieniu do jednostek pływających, w tym silników jednostek pływających, i statków powietrznych, w tym silników statków powietrznych, mają dostęp do następujących danych wprowadzonych do SIS zgodnie z art. 38 ust. 2 wyłącznie w celu sprawdzenia, czy jednostki pływające, w tym silniki jednostek pływających, oraz statki powietrzne, w tym silniki statków powietrznych, o których rejestrację zwrócono się do tych służb lub które podlegają zarządzaniu ruchem, zostały skradzione, przywłaszczone, utracone lub są poszukiwane jako dowód w postępowaniu karnym: a) dane dotyczące jednostek pływających; b) dane dotyczące silników jednostek pływających; c) dane dotyczące statków powietrznych; d) dane dotyczące silników statków powietrznych. Dostęp służb, o których mowa w akapicie pierwszym, do danych regulowany jest prawem krajowym i jest ograniczony do kompetencji szczególnej danych służb. 2. Służby, o których mowa w ust. 1, będące służbami państwowymi, mają prawo do bezpośredniego dostępu do danych w SIS.  3. Służby, o których mowa w ust. 1 niniejszego artykułu, niebędące służbami państwowymi, mają dostęp do danych w SIS wyłącznie za pośrednictwem organu, o którym mowa w art. 44. Organ ten ma prawo do bezpośredniego dostępu do danych i przekazywania ich odpowiednim służbom. Dane państwo członkowskie zapewnia, by przedmiotowe służby i ich pracownicy byli zobowiązani do przestrzegania wszelkich ograniczeń dotyczących dozwolonego wykorzystywania danych przekazywanych im przez ten organ.  4. Art. 39 nie ma zastosowania do dostępu do SIS uzyskanego zgodnie z niniejszym artykułem. Przekazywanie policji lub organom wymiaru sprawiedliwości przez służby, o których mowa w ust. 1 niniejszego artykułu, informacji uzyskanych w wyniku dostępu do SIS regulowane jest prawem krajowym. | **T** | Art. 1 pkt 5 | art. 4 otrzymuje brzmienie  (…)  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 samorządowym właściwym w sprawach rejestracji pojazdów.  3. Uprawnienie do bezpośredniego 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. h oraz i, przysługuje Prezesowi Urzędu Lotnictwa Cywilnego.**  4. 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, staroście lub właściwemu polskiemu związkowi sportowemu w rozumieniu ustawy z dnia 25 czerwca 2010 r. o sp**orcie (Dz. U. z 2020 r. poz. 1133).  5. 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 74 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2021 r. poz. 450, 463, 694 i 720) 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; |  |
|  | **Art. 47** | Artykuł 47  **Służby rejestrujące broń palną**  1. Służby w państwach członkowskich odpowiedzialne za wydawanie zaświadczeń dotyczących rejestracji broni palnej mają dostęp do danych dotyczących osób, wprowadzonych do SIS zgodnie z art. 26 i 36, oraz do danych dotyczących broni palnej, wprowadzonych do SIS zgodnie z art. 38 ust.  2. Z dostępu korzysta się na potrzeby sprawdzenia, czy osoba ubiegająca się o rejestrację jest osobą poszukiwaną w celu aresztowania i wydania lub aresztowania i ekstradycji albo do celów kontroli niejawnej, rozpytania kontrolnego lub kontroli szczególnej lub czy broń palna, o której zarejestrowanie wystąpiono, jest poszukiwana w celu zajęcia lub w celu wykorzystania jako dowód w postępowaniu karnym. 2. Dostęp służb, o których mowa w ust. 1, do danych regulowany jest prawem krajowym i jest ograniczony do kompetencji szczególnej danych służb.  3. Służby, o których mowa w ust. 1, będące służbami państwowymi, mają prawo do bezpośredniego dostępu do danych w SIS.  4. Służby, o których mowa w ust. 1, niebędące służbami państwowymi, mają dostęp do danych w SIS wyłącznie za pośrednictwem organu, o którym mowa w art. 44. Ten organ pośredniczący ma prawo do bezpośredniego dostępu do danych i informuje zainteresowane służby o tym, czy dana broń palna może zostać zarejestrowana. Dane państwo członkowskie zapewnia, by przedmiotowe służby i ich pracownicy byli zobowiązani do przestrzegania wszelkich ograniczeń dotyczących dozwolonego wykorzystywania danych przekazywanych im przez organ pośredniczący.  5. Art. 39 nie ma zastosowania do dostępu do SIS uzyskanego zgodnie z niniejszym artykułem. Przekazywanie policji lub organom wymiaru sprawiedliwości przez służby, o których mowa w ust. 1 niniejszego artykułu, informacji uzyskanych w wyniku dostępu do SIS regulowane jest prawem krajowym. | **T** | Art. 1 pkt 4 | Art. 3. Otrzymuje brzmienie  Uprawnienie do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów danych SIS dotyczących  (…)  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 prokuratorowi; |  |
|  | **Art. 48** | Artykuł 48  **Dostęp Europolu do danych SIS**  1. Jeżeli jest to niezbędne do wykonywania jej mandatu, Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), ustanowiona rozporządzeniem (UE) 2016/794, ma prawo do dostępu do danych w SIS i do ich wyszukiwania. Europol może także dokonywać wymiany informacji uzupełniających i występować z wnioskami o dalsze informacje uzupełniające zgodnie z zasadami zawartymi w podręczniku SIRENE.  2. Jeżeli podczas wyszukiwania Europol stwierdzi istnienie wpisu w SIS, informuje o tym – w drodze wymiany informacji uzupełniających przy użyciu infrastruktury łączności i zgodnie z zasadami zawartymi w podręczniku SIRENE – państwo członkowskie dokonujące wpisu. Dopóki Europol nie będzie w stanie korzystać z funkcji przewidzianych do wymiany informacji uzupełniających, w celu przekazywania informacji państwom członkowskim dokonującym wpisu wykorzystuje kanały określone w rozporządzeniu (UE) 2016/794.  3. Europol może przetwarzać informacje uzupełniające, które przekazały mu państwa członkowskie, do celów przeprowadzania porównań ze swoimi bazami danych i projektami analitycznymi, mających służyć wskazaniu powiązań lub innych odpowiednich związków, oraz do celów analiz strategicznych, tematycznych lub operacyjnych, o których mowa w art. 18 ust. 2 lit. a), b) i c) rozporządzenia (UE) 2016/794. Europol przetwarza informacje uzupełniające do celów niniejszego artykułu zgodnie z tym rozporządzeniem.  4. Wykorzystanie przez Europol informacji uzyskanych w wyniku wyszukiwania w SIS lub w wyniku przetwarzania informacji uzupełniających wymaga zgody państwa członkowskiego dokonującego wpisu. Jeżeli to państwo członkowskie zezwoli na wykorzystanie takich informacji, posługiwanie się nimi przez Europol regulowane jest rozporządzeniem (UE) 2016/794. Europol przekazuje takie informacje państwom trzecim i podmiotom trzecim wyłącznie za zgodą państwa członkowskiego dokonującego wpisu i z pełnym poszanowaniem prawa Unii dotyczącego ochrony danych.  5. Europol: a) bez uszczerbku dla ust. 4 i 6 nie podłącza części SIS ani nie przekazuje danych, które są w tych częściach zawarte i do których ma dostęp, do systemu gromadzenia i przetwarzania danych stosowanego przez Europol lub w Europolu, a także nie pobiera ani w inny sposób nie kopiuje części SIS; b) niezależnie od art. 31 ust. 1 rozporządzenia (UE) 2016/794 usuwa informacje uzupełniające zawierające dane osobowe najpóźniej rok po usunięciu związanego z nimi wpisu. Na zasadzie odstępstwa, jeżeli Europol posiada w swoich bazach danych lub projektach analitycznych informacje o sprawie, której dotyczą informacje uzupełniające, w celu wykonywania swoich zadań Europol może wyjątkowo w razie potrzeby nadal przechowywać te informacje uzupełniające. Europol informuje państwo członkowskie dokonujące wpisu i wykonujące państwo członkowskie o dalszym przechowywaniu takich informacji uzupełniających i przedstawia jego uzasadnienie; c) ogranicza dostęp do danych w SIS, w tym do informacji uzupełniających, tak by korzystali z niego tylko specjalnie uprawnieni pracownicy Europolu, którym dostęp do tych danych jest potrzebny do wykonywania ich zadań; d) przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13; e) zapewnia, by pracownicy uprawnieni do przetwarzania danych SIS przeszli odpowiednie szkolenie i zostali odpowiednio poinformowani zgodnie z art. 14 ust. 1; oraz f) bez uszczerbku dla rozporządzenia (UE) 2016/794 zapewnia Europejskiemu Inspektorowi Ochrony Danych możliwość monitorowania i kontrolowania działań podejmowanych przez Europol w ramach wykonywania prawa do dostępu do danych w SIS i ich wyszukiwania oraz w ramach wymiany i przetwarzania informacji uzupełniających.  6. Europol kopiuje dane z SIS wyłącznie do celów technicznych, jeżeli takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez należycie uprawnionych pracowników Europolu. Do takich kopii zastosowanie ma niniejsze rozporządzenie. Kopię techniczną wykorzystuje się do przechowywania danych SIS w trakcie przeprowadzania ich wyszukiwania. Po przeprowadzeniu wyszukiwania danych dane te są usuwane. Takich przypadków wykorzystywania danych nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie danych SIS. Europol nie kopiuje do innych systemów Europolu danych zawartych we wpisach lub danych dodatkowych wprowadzonych przez państwa członkowskie lub pochodzących z CS-SIS.  7. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europol rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS oraz każde wyszukiwanie w SIS. Prowadzenia takiej rejestracji i dokumentacji nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie części SIS. 8. Państwa członkowskie informują Europol w drodze wymiany informacji uzupełniających o każdym trafieniu odnoszącym się do wpisów dotyczących przestępstw terrorystycznych. Państwa członkowskie mogą w wyjątkowych okolicznościach nie przekazywać Europolowi takich informacji, jeżeli takie przekazanie mogłoby spowodować zagrożenie dla realizowanych czynności lub bezpieczeństwa osób lub byłoby sprzeczne z istotnymi interesami w zakresie bezpieczeństwa państwa członkowskiego dokonującego wpisu. 9. Ust. 8 stosuje się od daty, z którą Europol będzie w stanie otrzymywać informacje uzupełniające zgodnie z ust. 1. | **N** |  |  | Dotyczy Europolu. |
|  | **Art. 49** | Artykuł 49  **Dostęp Eurojustu do danych w SIS**  1. Wyłącznie przedstawiciele krajowi w Eurojuście oraz ich asystenci w ramach swojego mandatu mają prawo, jeśli jest to niezbędne do wykonywania ich mandatu, do dostępu do danych w SIS zgodnie z art. 26, 32, 34, 38 i 40 oraz do wyszukiwania tych danych.  2. Jeżeli w wyniku wyszukiwania przedstawiciel krajowy w Eurojuście stwierdzi istnienie wpisu w SIS, ów przedstawiciel krajowy powiadamia o tym państwo członkowskie dokonujące wpisu. Eurojust przekazuje informacje uzyskane w wyniku takiego wyszukiwania państwom trzecim i podmiotom trzecim wyłącznie za zgodą państwa członkowskiego dokonującego wpisu i z pełnym poszanowaniem prawa Unii dotyczącego ochrony danych.  3. Niniejszy artykuł pozostaje bez uszczerbku dla przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 ( 1 ) i rozporządzenia (UE) 2018/1725 dotyczących ochrony danych i odpowiedzialności za nieuprawnione lub nieprawidłowe przetwarzanie takich danych przez przedstawicieli krajowych w Eurojuście i ich asystentów oraz dla uprawnień Europejskiego Inspektora Ochrony Danych przewidzianych w tych rozporządzeniach.  4. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Eurojust rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS oraz każde wyszukiwanie w SIS przez przedstawiciela krajowego w Eurojuście lub przez jego asystenta.  5. Żadnych części SIS nie podłącza się do systemu gromadzenia i przetwarzania danych stosowanego przez Eurojust lub w Eurojuście, a danych w SIS, do których dostęp mają przedstawiciele krajowi lub ich asystenci, nie przekazuje się do takiego systemu. Nie można pobierać ani kopiować żadnych części SIS. Rejestrowania dostępu i wyszukiwania nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie danych SIS. 6. Eurojust przyjmuje i stosuje środki mające na celu zapewnienie bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13. | **N** |  |  | Dotyczy Agencji Eurojust. |
|  | **Art. 50** | Artykuł 50  **Dostęp zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członków zespołów wspierających zarządzanie migracjami do danych w SIS**  1. Zgodnie z art. 40 ust. 8 rozporządzenia (UE) 2016/1624 członkowie zespołów, o których mowa w art. 2 pkt 8 i 9 tego rozporządzenia, mają – w ramach swojego mandatu oraz pod warunkiem że są uprawnieni do przeprowadzania kontroli zgodnie z art. 44 ust. 1 niniejszego rozporządzenia i przeszli wymagane szkolenie zgodnie z art. 14 ust. 1 niniejszego rozporządzenia – prawo do dostępu do danych w SIS oraz do wyszukiwania takich danych w zakresie, w jakim jest to niezbędne do wykonywania ich zadań i zgodnie z wymogami planu operacyjnego dla danej operacji. Pozostali członkowie zespołów nie są uprawnieni do dostępu do danych w SIS.  2. Członkowie zespołów, o których mowa w ust. 1, wykonują prawo do dostępu do danych w SIS oraz do wyszukiwania takich danych zgodnie z ust. 1, korzystając z interfejsu technicznego. Interfejsu techniczny zostanie utworzony i będzie prowadzony przez Europejską Agencję Straży Granicznej i Przybrzeżnej i będzie umożliwiał bezpośrednie połączenie z systemem centralnym SIS. 3. Jeżeli w wyniku wyszukiwania członek zespołów, o których mowa w ust. 1 niniejszego artykułu, stwierdzi istnienie wpisu w SIS, powiadamia się o tym fakcie państwo członkowskie dokonujące wpisu. Zgodnie z art. 40 rozporządzenia (UE) 2016/1624 członkowie zespołów podejmują działania w odpowiedzi na wpis w SIS wyłącznie na polecenie i – co do zasady – w obecności funkcjonariuszy straży granicznej lub personelu realizującego zadania w dziedzinie powrotów z przyjmującego państwa członkowskiego, w którym działają. Przyjmujące państwo członkowskie może upoważnić członków zespołów do działania w jego imieniu.  4. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europejska Agencja Straży Granicznej i Przybrzeżnej rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS oraz każde wyszukiwanie w SIS.  5. Europejska Agencja Straży Granicznej i Przybrzeżnej przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13 oraz zapewnia, by zespoły, o których mowa w ust. 1 niniejszego artykułu, stosowały te środki.  6. Przepisów niniejszego artykułu nie można interpretować jako mających wpływ na przepisy rozporządzenia (UE) 2016/1624 dotyczące ochrony danych i odpowiedzialności Europejskiej Agencji Straży Granicznej i Przybrzeżnej za nieuprawnione lub nieprawidłowe przetwarzanie danych. L 312/88 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 ( 1 ) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.U. L 295 z 21.11.2018, s. 138).  7. Bez uszczerbku dla ust. 2 żadnych części SIS nie podłącza się do systemu gromadzenia i przetwarzania danych stosowanego przez zespoły, o których mowa w ust. 1, lub przez Europejską Agencję Straży Granicznej i Przybrzeżnej, a danych w SIS, do których dostęp mają te zespoły, nie przekazuje się do takiego systemu. Nie można pobierać ani kopiować żadnych części SIS. Rejestrowania dostępu i wyszukiwania nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie danych SIS.  8. Europejska Agencja Straży Granicznej i Przybrzeżnej zapewnia Europejskiemu Inspektorowi Ochrony Danych możliwość monitorowania i kontrolowania działań prowadzonych przez zespoły, o których mowa w niniejszym artykule, w ramach wykonywania ich prawa do dostępu do danych w SIS i wyszukiwania takich danych. Pozostaje to bez uszczerbku dla dalszych przepisów rozporządzenia (UE) 2018/1725. | **N** |  |  | Dotyczy Agencji Europejskiej Straży Granicznej i Przybrzeżnej (Frontex), zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członków zespołów wspierających zarządzanie migracjami do danych w SIS |
|  | **Art. 51** | Artykuł 51  **Ocena użytkowania SIS przez Europol, Eurojust oraz Europejską Agencję Straży Granicznej i Przybrzeżnej**  1. Co najmniej raz na pięć lat Komisja przeprowadza ocenę eksploatowania i użytkowania SIS przez Europol, przedstawicieli krajowych w Eurojuście i ich asystentów oraz zespoły, o których mowa w art. 50 ust. 1.  2. Europol, Eurojust i Europejska Agencja Straży Granicznej i Przybrzeżnej zapewniają podjęcie odpowiednich działań następczych w związku z ustaleniami i zaleceniami wynikającymi z tej oceny.  3. Sprawozdanie na temat wyników oceny i podjętych działań następczych przekazuje się Parlamentowi Europejskiemu i Radzie. | **N** |  |  | Ewaluację przeprowadza Komisja Europejska. |
|  | **Art. 52** | Artykuł 52  **Zakres dostępu**  Użytkownicy końcowi, w tym Europol, przedstawiciele krajowi w Eurojuście i ich asystenci oraz członkowie zespołów, o których mowa w art. 2 pkt 8 i 9 rozporządzenia (UE) 2016/1624, mają dostęp wyłącznie do tych danych, które są im niezbędne do wykonywania ich zadań. | **N** |  |  | Techniczne warunki stosowania przepisu zapewnia Agencja eu-LISA (odpowiadająca za C.SIS). |
|  | **Art. 53** | Artykuł 53  **Termin weryfikacji wpisów dotyczących osób**  1. Wpisy dotyczące osób utrzymywane są wyłącznie przez czas konieczny do osiągnięcia celów, do których zostały wprowadzone.  2. Państwo członkowskie może wprowadzić wpis dotyczący osoby do celów art. 26 i art. 32 ust. 1 lit. a) i b)na okres pięciu lat. W tym pięcioletnim okresie państwo członkowskie dokonujące wpisu weryfikuje, czy istnieje potrzeba jego dalszego utrzymywania.  3. Państwo członkowskie może wprowadzić wpis dotyczący osoby do celów art. 34 i 40 na okres trzech lat. W tym trzyletnim okresie państwo członkowskie dokonujące wpisu weryfikuje, czy istnieje potrzeba jego dalszego utrzymywania.  4. Państwo członkowskie może wprowadzić wpis dotyczący osoby do celów art. 32 ust. 1 lit. c), d) i e) oraz art. 36 na okres jednego roku. W tym rocznym okresie państwo członkowskie dokonujące wpisu weryfikuje, czy istnieje potrzeba jego dalszego utrzymywania.  5. Każde państwo członkowskie ustanawia w stosownych przypadkach krótsze terminy weryfikacji, zgodnie ze swoim prawem krajowym.  6. Przed upływem terminu weryfikacji, o którym mowa w ust. 2, 3 i 4, państwo członkowskie dokonujące wpisu może, na podstawie wszechstronnej indywidualnej oceny, która podlega zarejestrowaniu, podjąć decyzję o utrzymywaniu wpisu po upływie terminu weryfikacji, jeżeli jest to niezbędne i proporcjonalne do celów, do których wprowadzono ten wpis. W takich przypadkach ust. 2, 3 lub 4 mają zastosowanie również do przedłużenia okresu utrzymywania wpisu. Informacje o takim przedłużeniu są przekazywane do CS-SIS.  7. Po upływie terminu weryfikacji, o którym mowa w ust. 2, 3 i 4, wpisy dotyczące osób usuwane są automatycznie, z wyjątkiem przypadków, gdy państwo członkowskie dokonujące wpisu poinformowało CS-SIS o przedłużeniu okresu utrzymywania wpisu zgodnie z ust. 6. CS-SIS automatycznie informuje państwo członkowskie dokonujące wpisu z czteromiesięcznym wyprzedzeniem o zaplanowanym usunięciu danych z systemu.  8. Państwa członkowskie prowadzą statystyki na temat liczby wpisów dotyczących osób, w przypadku których okres utrzymywania został przedłużony zgodnie z ust. 6 niniejszego artykułu i przekazują je organom nadzorczym, o których mowa w art. 69, na ich wniosek. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/89  9. Jak tylko dla biura SIRENE stanie się jasne, że wpis dotyczący danej osoby spełnił swój cel i powinien w związku z tym zostać usunięty, natychmiast powiadamia ono o tym organ, który utworzył wpis. W terminie 15 dni kalendarzowych od otrzymania takiego powiadomienia organ ten informuje, że wpis został usunięty lub ma zostać usunięty, lub przedstawia powody dalszego utrzymywania wpisu. Jeżeli organ nie udzieli takiej odpowiedzi w terminie 15 dni, biuro SIRENE zapewnia, by wpis został usunięty. Jeżeli jest to dopuszczalne na mocy prawa krajowego, wpis jest usuwany przez biuro SIRENE. Biura SIRENE zgłaszają swojemu organowi nadzorczemu powtarzające się problemy, które napotkały działając na podstawie niniejszego ustępu. | **T** | Art. 1 pkt 14  Art. 1 pkt 4 | Pkt 14:  art. 27 otrzymuje brzmienie:  (…)  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**.”;  Pkt 4  Art. 3 ust 3 otrzymuje brzmienie  (…)  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 ust. 7, art. 40 i art. 44 rozporządzenia 2018/1861 oraz art. 53 ust. 1–7 i ust. 9, art. 54 ust. 1–4, art. 55 i art. 59 rozporządzenia 2018/1862.. |  |
|  | **Art. 54** | Artykuł 54  **Termin weryfikacji wpisów dotyczących przedmiotów**  1. Wpisy dotyczące przedmiotów utrzymywane są wyłącznie przez czas konieczny do osiągnięcia celów, do których zostały wprowadzone.  2. Państwo członkowskie może wprowadzić wpis dotyczący przedmiotu do celów art. 36 i 38 na okres dziesięciu lat. W tym dziesięcioletnim okresie państwo członkowskie dokonujące wpisu weryfikuje, czy istnieje potrzeba jego dalszego utrzymywania.  3. Wpisy dotyczące przedmiotów wprowadzone zgodnie z art. 26, 32, 34 i 36 podlegają weryfikacji zgodnie z art. 53, w przypadku gdy istnieje odsyłacz między nimi a wpisem dotyczącym osoby. Wpisy takie są utrzymywane wyłącznie przez okres, przez jaki utrzymywany jest ten wpis dotyczący osoby.  4. Przed upływem terminu weryfikacji, o którym mowa w ust. 2 i 3, państwo członkowskie dokonujące wpisu może podjąć decyzję o utrzymywaniu wpisu dotyczącego przedmiotu po upływie terminu weryfikacji, jeżeli jest to niezbędne do celów, do których wprowadzono ten wpis. W takich przypadkach zastosowanie mają odpowiednio ust. 2 lub 3.  5. Komisja może przyjąć akty wykonawcze w celu określenia krótszych terminów weryfikacji w odniesieniu do niektórych kategorii wpisów dotyczących przedmiotów. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2.  6. Państwa członkowskie prowadzą statystyki na temat liczby tych wpisów dotyczących przedmiotów, w przypadku których okres przechowywania został przedłużony zgodnie z ust. 4. | **T** | Art. 1 pkt 14  Art. 1 pkt 4 | Pkt 14:  art. 27 otrzymuje brzmienie:  (…)  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**.”;  Pkt 4  Art. 3 ust 3 otrzymuje brzmienie  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 ust. 7, art. 40 i art. 44 rozporządzenia 2018/1861 oraz art. 53 ust. 1–7 i ust. 9, art. 54 ust. 1–4, art. 55 i art. 59 rozporządzenia 2018/1862. | Art. 54 ust. 5 nie wymaga transpozycji. |
|  | **Art. 55** | Artykuł 55  **Usuwanie wpisów**  1. Wpisy mające doprowadzić do aresztowania osób w celu ich wydania lub ekstradycji, dokonane zgodnie z art. 26, usuwa się po wydaniu lub ekstradycji danej osoby właściwym organom państwa członkowskiego dokonującego wpisu. Wpisy usuwa się również w przypadku uchylenia przez właściwy organ wymiaru sprawiedliwości zgodnie z prawem krajowym decyzji wydanej przez organ wymiaru sprawiedliwości, która stanowi podstawę wpisu. Wpisy są również usuwane po wygaśnięciu wpisu zgodnie z art. 53.  2. Wpisy dotyczące osób zaginionych lub osób narażonych na niebezpieczeństwo, którym należy uniemożliwić podróżowanie, dokonane zgodnie z art. 32, usuwa się zgodnie z następującymi zasadami: a) w przypadku zaginionych dzieci i dzieci zagrożonych uprowadzeniem wpis usuwa się w następstwie: (i) rozwiązania sprawy, np. jeżeli dziecko zostało zlokalizowane lub poddane repatriacji lub jeżeli właściwe organy w wykonującym państwie członkowskim podjęły decyzję dotyczącą opieki nad dzieckiem; (ii) wygaśnięcia wpisu zgodnie z art. 53; lub (iii) decyzji właściwego organu państwa członkowskiego dokonującego wpisu; b) w przypadku zaginionych osób dorosłych – jeżeli nie wystąpiono o środki ochrony – wpis usuwa się w następstwie: (i) wykonania działania, które miało zostać przeprowadzone, w przypadku gdy wykonujące państwo członkowskie ustaliło miejsce pobytu; (ii) wygaśnięcia wpisu zgodnie z art. 53; lub (iii) decyzji właściwego organu państwa członkowskiego dokonującego wpisu; c) w przypadku zaginionych osób dorosłych – jeżeli wystąpiono o środki ochrony – wpis usuwa się w następstwie: (i) wykonania działania, które miało zostać przeprowadzone, w przypadku gdy dana osoba została objęta ochroną; L 312/90 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 (ii) wygaśnięcia wpisu zgodnie z art. 53; lub (iii) decyzji właściwego organu państwa członkowskiego dokonującego wpisu. d) w przypadku osób pełnoletnich narażonych na niebezpieczeństwo, którym dla ich własnej ochrony należy uniemożliwić podróżowanie, i w przypadku dzieci, którym należy uniemożliwić podróżowanie, wpis usuwa się w następstwie: (i) wykonania działania, które miało zostać przeprowadzone, takiego jak objęcie osoby ochroną; (ii) wygaśnięcia wpisu zgodnie z art. 53; lub (iii) decyzji właściwego organu państwa członkowskiego dokonującego wpisu. Bez uszczerbku dla prawa krajowego, jeżeli osoba została przymusowo umieszczona w odpowiedniej placówce w następstwie decyzji podjętej przez właściwy organ, wpis można utrzymywać do czasu repatriacji tej osoby.  3. Wpisy dotyczące osób poszukiwanych na potrzeby postępowania prowadzonego przez organy wymiaru sprawiedliwości na podstawie art. 34 usuwa się w następstwie: a) przekazania informacji o miejscu pobytu osoby właściwemu organowi państwa członkowskiego dokonującego wpisu; b) wygaśnięcia wpisu zgodnie z art. 53; lub c) decyzji właściwego organu państwa członkowskiego dokonującego wpisu. Jeżeli nie można podjąć działań w związku z przekazanymi informacjami, o których mowa w lit. a), biuro SIRENE państwa członkowskiego dokonującego wpisu powiadamia biuro SIRENE wykonującego państwa członkowskiego w celu rozwiązania problemu. W przypadku trafienia, jeżeli dane adresowe zostały przekazane państwu członkowskiemu dokonującemu wpisu, a kolejne trafienie w tym samym wykonującym państwie członkowskim wskazuje te same dane adresowe, trafienie rejestruje się w wykonującym państwie członkowskim, przy czym państwu członkowskiemu dokonującemu wpisu nie przesyła się ponownie ani danych adresowych, ani informacji uzupełniających. W takich przypadkach wykonujące państwo członkowskie informuje państwo członkowskie dokonujące wpisu o powtarzających się trafieniach, a państwo członkowskie dokonujące wpisu przeprowadza wszechstronną indywidualną ocenę konieczności utrzymania wpisu.  4. Wpisy dotyczące kontroli niejawnych, rozpytań kontrolnych i kontroli szczególnych na podstawie art. 36 usuwa się w następstwie: a) wygaśnięcia wpisu zgodnie z art. 53; lub b) decyzji o ich usunięciu podjętej przez właściwy organ państwa członkowskiego dokonującego wpisu. 5. Wpisy dotyczące przedmiotów podlegających zajęciu lub przeznaczonych do wykorzystania jako dowód w postępowaniu karnym na podstawie art. 38 usuwa się w następstwie: a) zajęcia przedmiotu lub podjęcia równoważnego środka po przeprowadzeniu niezbędnych działań następczych w zakresie wymiany informacji uzupełniających między odpowiednimi biurami SIRENE lub po tym, jak przedmiot zostanie objęty inną procedurą prowadzoną przez organy wymiaru sprawiedliwości lub procedurą administracyjną; b) wygaśnięcia wpisu zgodnie z art. 53; lub c) decyzji o ich usunięciu podjętej przez właściwy organ państwa członkowskiego dokonującego wpisu.  6. Wpisy dotyczące nieznanych osób poszukiwanych, dokonane zgodnie z art. 40, usuwa się w następstwie: a) zidentyfikowania osoby; b) wygaśnięcia wpisu zgodnie z art. 53; lub c) podjęcia przez właściwy organ państwa członkowskiego dokonującego wpisu decyzji o ich usunięciu.  7. W przypadku istnienia odsyłacza między danym wpisem a wpisem dotyczącym osoby, wpisy dotyczące przedmiotów wprowadzone zgodnie z art. 26, 32, 34 i 36 usuwa się w momencie usunięcia wpisu dotyczącego tej osoby zgodnie z niniejszym artykułem. | **T** | Art. 1 pkt 4 | Art. 3 ust 3 otrzymuje brzmienie  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 ust. 7, art. 40 i art. 44 rozporządzenia 2018/1861 oraz art. 53 ust. 1–7 i ust. 9, art. 54 ust. 1–4, art. 55 i art. 59 rozporządzenia 2018/1862. |  |
|  | **Art. 56** | Artykuł 56  **Przetwarzanie danych SIS**  1. Państwa członkowskie przetwarzają dane, o których mowa w art. 20, wyłącznie do celów określonych dla każdej z kategorii wpisu, o których mowa w art. 26, 32, 34, 36, 38 i 40.  2. Dane są kopiowane wyłącznie do celów technicznych, jeżeli takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez właściwe organy, o których mowa w art. 44. Do takich kopii zastosowanie ma niniejsze rozporządzenie. Państwo członkowskie nie kopiuje – do innych krajowych plików danych – danych zawartych we wpisie ani danych dodatkowych wprowadzonych przez inne państwo członkowskie z N.SIS tego państwa lub z CSSIS. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/91 3. Kopie techniczne, o których mowa w ust. 2, przekształcane w bazy danych działające w trybie offline, mogą być przechowywane przez okres nieprzekraczający 48 godzin. Państwa członkowskie prowadzą aktualny spis takich kopii, który udostępniają swoim organom nadzorczym, oraz zapewniają, by w odniesieniu do tych kopii stosowane było niniejsze rozporządzenie, w szczególności art. 10.  4. Właściwe organy krajowe, o których mowa w art. 34, uzyskują dostęp do danych w SIS wyłącznie w granicach swoich kompetencji i jest on przyznawany wyłącznie należycie uprawnionym pracownikom.  5. W odniesieniu do wpisów, o których mowa w art. 26, 32, 34, 36, 38 i 40 niniejszego rozporządzenia, każdy przypadek przetwarzania informacji w SIS do celów innych niż te, w których informacje te zostały wprowadzone do SIS, musi być związany z konkretną sprawą i uzasadniony potrzebą zapobieżenia bezpośredniemu poważnemu zagrożeniu dla porządku publicznego i bezpieczeństwa publicznego, poważnymi względami bezpieczeństwa narodowego lub koniecznością zapobieżenia poważnemu przestępstwu. W tym celu uprzednio uzyskuje się zgodę państwa członkowskiego dokonującego wpisu. 6. Każdy przypadek wykorzystania danych SIS w sposób niezgodny z ust. 1–5 niniejszego artykułu uznaje się za wykorzystanie tych danych niezgodnie z przeznaczeniem w świetle prawa krajowego poszczególnych państw członkowskich i podlega on sankcjom zgodnie z art. 73.  7. Każde państwo członkowskie przekazuje eu-LISA wykaz swoich właściwych organów, które są uprawnione do przeprowadzania wyszukiwania danych bezpośrednio w SIS zgodnie z niniejszym rozporządzeniem, jak również wszelkie zmiany dotyczące tego wykazu. Wykaz ten określa – w odniesieniu do każdego organu – jakie dane mogą być wyszukiwane i w jakich celach. eu-LISA zapewnia coroczną publikację wykazu w Dzienniku Urzędowym Unii Europejskiej. eu-LISA prowadzi na swojej stronie internetowej stale aktualizowany wykaz zawierający zmiany przekazane przez państwa członkowskie w okresie pomiędzy corocznymi publikacjami.  8. Jeżeli prawo Unii nie zawiera przepisów szczegółowych, do danych w N.SIS zastosowanie mają przepisy poszczególnych państw członkowskich. | **T** | Art. 1 pkt 14 | Art. 27. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 2, centralny organ techniczny KSI jest obowiązany do:  6) przekazywania organowi zarządzającemu systemem centralnym SIS wykazu organów, o których mowa w art. 3 ust. 1 i art. 4 ust. 1 i 3 oraz zmian w tym zakresie; | W zakresie art. 56 ust. 1-6 oraz ust. 8 rozporządzenie nie wymaga transpozycji. |
|  | **Art. 57** | Artykuł 57  **Dane SIS i pliki krajowe**  1. Art. 56 ust. 2 pozostaje bez uszczerbku dla prawa państwa członkowskiego do utrzymywania w swoich plikach krajowych danych SIS, w związku z którymi podjęto działanie na jego terytorium. Takie dane są utrzymywane w plikach krajowych przez okres nie dłuższy niż trzy lata, chyba że przepisy szczegółowe prawa krajowego przewidują dłuższy okres ich utrzymywania.  2. Art. 56 ust. 2 pozostaje bez uszczerbku dla prawa państwa członkowskiego do utrzymywania w swoich plikach krajowych danych zawartych w konkretnym wpisie wprowadzonym do SIS przez to państwo członkowskie. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości. |
|  | **Art. 58** | Artykuł 58  **Poinformowanie o niewykonywaniu wpisu**  Jeżeli wymagane działanie nie może zostać wykonane, wezwane do działania państwo członkowskie natychmiast informuje o tym – w drodze wymiany informacji uzupełniających – państwo członkowskie dokonujące wpisu. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości. |
|  | **Art. 59** | Artykuł 59  **Jakość danych w SIS**  1. Państwo członkowskie dokonujące wpisu odpowiada za zapewnienie, by dane były prawidłowe, aktualne i wprowadzane do SIS oraz przechowywane w SIS zgodnie z prawem.  2. Jeżeli państwo członkowskie dokonujące wpisu uzyska odpowiednie dodatkowe lub zmienione dane wymienione w art. 20 ust. 3, niezwłocznie uzupełnia lub zmienia odnośny wpis.  3. Do zmiany, uzupełniania, korekty, aktualizacji lub usuwania danych wprowadzonych do SIS uprawnione jest wyłącznie państwo członkowskie dokonujące wpisu.  4. Jeżeli państwo członkowskie inne niż państwo członkowskie dokonujące wpisu posiada stosowne dodatkowe lub zmienione dane wymienione w art. 20 ust. 3, niezwłocznie przekazuje je – w drodze wymiany informacji uzupełniających – państwu członkowskiemu dokonującemu wpisu, tak by mogło ono uzupełnić lub zmienić wpis. Jeżeli te dodatkowe lub zmienione dane dotyczą osób, przekazywane są wyłącznie w przypadkach gdy tożsamość danej osoby została ustalona. 5. Jeżeli państwo członkowskie inne niż państwo dokonujące wpisu posiada dowody wskazujące, że jeden z elementów danych jest niezgodny ze stanem faktycznym lub jest przechowywany niezgodnie z prawem, informuje o tym – w drodze wymiany informacji uzupełniających – państwo członkowskie dokonujące wpisu, jak najszybciej i nie później niż dwa dni robocze po stwierdzeniu istnienia takich dowodów. Państwo członkowskie dokonujące wpisu sprawdza te informacje oraz, w razie konieczności, niezwłocznie koryguje lub usuwa zakwestionowany element danych. L 312/92 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018  6. Jeżeli państwa członkowskie nie są w stanie osiągnąć porozumienia w terminie dwóch miesięcy od stwierdzenia istnienia dowodów, o których mowa w ust. 5 niniejszego artykułu, państwo członkowskie, które nie wprowadziło wpisu, przekazuje sprawę w drodze współpracy zgodnie z art. 71 odpowiednim organom nadzorczym i Europejskiemu Inspektorowi Ochrony Danych, którzy podejmują decyzję.  7. Jeżeli dana osoba twierdzi, że nie jest osobą, której ma dotyczyć, państwa członkowskie przeprowadzają wymianę informacji uzupełniających. Jeżeli w wyniku sprawdzenia okaże się, że wnoszący skargę nie jest osobą, której ma dotyczyć wpis, zostaje on powiadomiony o środkach określonych w art. 62 i o przysługującym mu środku ochrony prawnej zgodnie z art. 68 ust. 1. | **T** | Art. 1 pkt 4  Art. 1 pkt 7 | Art. 3 otrzymuje brzmienie  (…)  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 ust. 7, art. 40 i art. 44 rozporządzenia 2018/1861 oraz art. 53 ust. 1–7 i ust. 9, art. 54 ust. 1–4, art. 55 i art. 59 rozporządzenia 2018/1862.  Art. 9 otrzymuje brzmienie:  „Art. 9. Prezes Urzędu Ochrony Danych Osobowych w przypadku, o którym mowa w art. 44 ust. 6 rozporządzenia 2018/1861 oraz w **art. 59 ust. 6 rozporządzenia 2018/1862**, jest organem uprawnionym do przekazania sprawy Europejskiemu Inspektorowi Ochrony Danych, w celu podjęcia działań mediacyjnych.”; | Zmiana podstawy prawnej funkcjonowania systemu SIS oraz modyfikacja procedur związanych z realizacją operacji w nim przez organy krajowe. |
|  | **Art. 60** | Artykuł 60  **Incydenty bezpieczeństwa**  1. Każde zdarzenie, które ma lub może mieć wpływ na bezpieczeństwo SIS lub może spowodować uszkodzenie lub utratę danych SIS lub informacji uzupełniających, uznaje się za incydent bezpieczeństwa, w szczególności jeżeli mogło dojść do uzyskania niezgodnego z prawem dostępu do danych lub jeżeli zostały lub mogły zostać naruszone dostępność, integralność i poufność danych.  2. Incydentami bezpieczeństwa zarządza się w sposób zapewniający szybkie, skuteczne i właściwe reagowanie.  3. Bez uszczerbku dla zgłaszania naruszenia ochrony danych osobowych i zawiadamiania o takim naruszeniu zgodnie z art. 33 rozporządzenia (UE) 2016/679 lub art. 30 dyrektywy (UE) 2016/680, państwa członkowskie, Europol, Eurojust oraz Europejska Agencja Straży Granicznej i Przybrzeżnej niezwłocznie powiadamiają Komisję, eu-LISA, właściwy organ nadzorczy i Europejskiego Inspektora Ochrony Danych o incydentach bezpieczeństwa. eu-LISA niezwłocznie powiadamia Komisję i Europejskiego Inspektora Ochrony Danych o każdym incydencie bezpieczeństwa dotyczącym systemu centralnego SIS.  4. Informacje o incydencie bezpieczeństwa, który ma lub może mieć wpływ na funkcjonowanie SIS w państwie członkowskim lub w eu-LISA lub który ma lub może mieć wpływ na dostępność, integralność i poufność danych wprowadzonych lub przesłanych przez inne państwa członkowskie lub na informacje uzupełniające podlegające wymianie, są niezwłocznie przekazywane wszystkim państwom członkowskim i zgłaszane zgodnie z opracowanym przez eu-LISA planem zarządzania na wypadek incydentów bezpieczeństwa.  5. Państwa członkowskie i eu-LISA współpracują ze sobą w przypadku wystąpienia incydentu bezpieczeństwa. 6. Komisja natychmiast informuje o poważnych incydentach Parlament Europejski i Radę. Informacje takie opatrywane są klauzulą EU RESTRICTED/RESTREINT UE, zgodnie z mającymi zastosowanie przepisami bezpieczeństwa.  7. Jeżeli incydent bezpieczeństwa jest spowodowany wykorzystaniem danych niezgodnie z przeznaczeniem, państwa członkowskie, Europol, Eurojust oraz Europejska Agencja Straży Granicznej i Przybrzeżnej zapewniają zastosowanie sankcji zgodnie z art. 73. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości. |
|  | **Art. 61** | Artykuł 61  **Rozróżnianie osób o podobnych cechach**  1. W przypadku stwierdzenia przy wprowadzaniu nowego wpisu, że w SIS istnieje już wpis dotyczący osoby z takim samym opisem tożsamości, biuro SIRENE w terminie 12 godzin zwraca się w drodze wymiany informacji uzupełniających do państwa członkowskiego dokonującego wpisu o wyjaśnienie, czy wpisy dotyczą tej samej osoby.  2. Jeżeli w wyniku sprawdzania krzyżowego okaże się, że osoba, której dotyczy nowy wpis, oraz osoba, której dotyczy wpis wprowadzony wcześniej do SIS, to rzeczywiście ta sama osoba, biuro SIRENE stosuje procedurę wprowadzania wielokrotnych wpisów, o której mowa w art. 23.  3. Jeżeli w wyniku sprawdzenia okaże się, że chodzi faktycznie o dwie różne osoby, biuro SIRENE zatwierdza wniosek o wprowadzenie drugiego wpisu, dodając dane niezbędne do zapobieżenia błędnej identyfikacji. | **T** | Art. 1 pkt 5 | Art. 4 otrzymuje brzmienie  (…)  8. 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, o których mowa w ust. 1–4, z centralnym organem technicznym KSI oraz biurem SIRENE, w tym procedurę wymiany informacji uzupełniających określonych w art. 37 ust. 2 niezbędnych do wykonania wnioskowanych we wpisie działań, uwzględniając sprawną i skuteczną realizację wnioskowanych we wpisie działań wobec **odnalezionych osób lub przedmiotów.** | Uaktualnienie delegacji ustawowej w związku z brzmieniem art. 46 rozporządzenia 2018/1861 **o**raz **art. 61 rozporządzenia 2018/1862** poprzez rozszerzenie trybu i zasad współpracy organów uprawnionych z biurem SIRENE. |
|  | **Art. 62** | Artykuł 62  **Dane dodatkowe wprowadzane w celu rozwiązywania problemów związanych z przywłaszczaniem tożsamości**  1. Jeżeli istnieje ryzyko pomylenia osoby, której ma dotyczyć wpis, z osobą, której tożsamość została przywłaszczona, państwo członkowskie dokonujące wpisu uzupełnia wpis, za wyraźną zgodą osoby, której tożsamość została przywłaszczona, o dotyczące jej dane w celu zapobieżenia negatywnym skutkom błędnej identyfikacji. Osoba, której tożsamość została przywłaszczona, ma prawo do wycofania swojej zgody na przetwarzanie takich dodanych danych osobowych. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/93 2. Dane osoby, której tożsamość została przywłaszczona, wykorzystywane są wyłącznie w celach: a) umożliwienia właściwemu organowi odróżnienia osoby, której tożsamość została przywłaszczona, od osoby, której ma dotyczyć wpis; oraz b) umożliwienia osobie, której tożsamość została przywłaszczona, udowodnienia swojej tożsamości i wykazania, że jej tożsamość została przywłaszczona.  3. Na użytek niniejszego artykułu i pod warunkiem uzyskania wyraźnej zgody osoby, której tożsamość została przywłaszczona, w odniesieniu do każdej kategorii danych, wprowadzane do SIS i dalej w nim przetwarzane mogą być wyłącznie następujące dane osobowe osoby, której tożsamość została przywłaszczona: a) nazwiska; b) imiona; c) imiona i nazwiska nadane przy urodzeniu; d) poprzednio używane imiona i nazwiska oraz pseudonimy, w miarę możliwości wpisane oddzielnie; e) szczególne obiektywne cechy fizyczne niepodlegające zmianom; f) miejsce urodzenia; g) data urodzenia; h) płeć; i) fotografie i wizerunki twarzy; j) odbitki linii papilarnych palców, odbitki linii papilarnych dłoni lub odbitki linii papilarnych palców oraz dłoni; k) wszelkie posiadane obywatelstwa; l) kategoria dokumentów identyfikacyjnych danej osoby; m) państwo wydania dokumentów identyfikacyjnych danej osoby; n) numer lub numery dokumentów identyfikacyjnych danej osoby; o) data wydania dokumentów identyfikacyjnych danej osoby; p) adres danej osoby; q) imię i nazwisko ojca danej osoby; r) imię i nazwisko matki danej osoby.  4. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych niezbędnych do wprowadzania i dalszego przetwarzania danych, o których mowa w ust. 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2.  5. Dane, o których mowa w ust. 3, są usuwane w tym samym czasie, co odpowiadający im wpis, lub wcześniej, jeśli dana osoba o to wystąpi.  6. Dostęp do danych, o których mowa w ust. 3, mogą uzyskać wyłącznie organy mające prawo do dostępu do wpisu odpowiadającego tym danym. Mogą one z niego korzystać wyłącznie w celu zapobieżenia błędnej identyfikacji. | **T** | Art 1 pkt 2  Art. 1 pkt 5 | lit. f)  w pkt 19 kropkę zastępuje się średnikiem i dodaje się pkt 20–27 w brzmieniu: (…)  „21) tożsamości przywłaszczonej – rozumie się przez to dane wprowadzone do SIS zgodnie z art. 47 rozporządzenia 2018/1861 oraz zgodnie z **art. 62 rozporządzenia 2018/1862** dotyczące osoby pokrzywdzonej, której tożsamością posługuje się osoba poszukiwana na podstawie wpisu do SIS;  Art. 4 otrzymuje brzmienie  (…)  8. 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, o których mowa w ust. 1–4, z centralnym organem technicznym KSI oraz biurem SIRENE, w tym procedurę wymiany informacji uzupełniających określonych w art. 37 ust. 2 niezbędnych do wykonania wnioskowanych we wpisie działań, uwzględniając sprawną i skuteczną realizację wnioskowanych we wpisie działań wobec odnalezionych osób lub przedmiotów. | Uaktualnienie definicji w ustawie  w związku z brzmieniem **art. 62 rozporządzenia 2018/1862** poprzez rozszerzenie trybu i zasad współpracy organów uprawnionych z biurem SIRENE w zakresie rozwiązywania problemów związanych z przewłaszczaniem tożsamości.  Art. 62 ust. 4 nie wymaga transpozycji. |
|  | **Art. 63** | Artykuł 63  **Odsyłacze pomiędzy wpisami**  1. Państwo członkowskie może utworzyć odsyłacz pomiędzy wpisami, które wprowadza do SIS. Celem utworzenia takiego odsyłacza jest ustanowienie związku między dwoma wpisami lub większą liczbą wpisów.  2. Utworzenie odsyłacza nie wpływa na konkretne działanie, które ma zostać podjęte na podstawie każdego z tak powiązanych wpisów, ani na termin weryfikacji każdego z tak powiązanych wpisów.  3. Utworzenie odsyłacza nie wpływa na prawa do dostępu przewidziane w niniejszym rozporządzeniu. Organy nieposiadające prawa do dostępu do niektórych kategorii wpisów nie mogą widzieć odsyłacza do wpisu, do którego nie mają dostępu.  4. Państwo członkowskie tworzy odsyłacz pomiędzy wpisami, jeżeli jest to uzasadnione potrzebą operacyjną.  5. Jeżeli państwo członkowskie uzna, że utworzenie przez inne państwo członkowskie odsyłacza pomiędzy wpisami jest niezgodne z jego prawem krajowym lub zobowiązaniami międzynarodowymi, może podjąć niezbędne środki, by uniemożliwić dostęp do tego odsyłacza ze swojego terytorium lub uniemożliwić dostęp do tego odsyłacza swoim organom znajdującym się poza jego terytorium. L 312/94 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018  6. Komisja przyjmuje akty wykonawcze w celu określenia i rozwijania przepisów technicznych dotyczących tworzenia odsyłaczy między wpisami. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **T** | Art. 1 pkt 2  Art. 1 pkt 8 | lit. f)  w pkt 19 kropkę zastępuje się średnikiem i dodaje się pkt 20–27 w brzmieniu:  (…)  22) odsyłaczu – rozumie się przez to odsyłacz, o którym mowa w art. 48 rozporządzenia 2018/1861 i **art. 63 rozporządzenia 2018/1862**, utworzony w SIS pomiędzy co najmniej dwoma wpisami;  8) w art. 21 ust. 1 otrzymuje brzmienie:  „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 SIS**, 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.”; | Uaktualnienie definicji w ustawie  w związku z brzmieniem **art. 63 rozporządzenia 2018/1862** poprzez rozszerzenie trybu i zasad współpracy organów uprawnionych z biurem SIRENE w zakresie rozwiązywania problemów związanych z tworzeniem odsyłaczy pomiędzy wpisami.  Art. 63 ust. 6 nie wymaga transpozycji. |
|  | **Art. 64** | Artykuł 64  **Cel i okres przechowywania informacji uzupełniających**  1. Państwa członkowskie przechowują odniesienia do decyzji, które są podstawą wpisu, w biurze SIRENE w celu ułatwienia wymiany informacji uzupełniających.  2. Dane osobowe, które biuro SIRENE przechowuje w plikach w wyniku wymiany informacji, utrzymywane są wyłącznie przez okres wymagany do osiągnięcia celów, w których zostały dostarczone. Są one usuwane najpóźniej rok po usunięciu z SIS związanego z nimi wpisu.  3. Ust. 2 pozostaje bez uszczerbku dla prawa państwa członkowskiego do utrzymywania w plikach krajowych danych dotyczących konkretnego wprowadzonego przez nie, wpisu lub wpisu, w związku z którym podjęto działanie na jego terytorium. Okres przechowywania takich danych w takich plikach reguluje prawo krajowe. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości. |
|  | **Art. 65** | Artykuł 65  **Przekazywanie danych osobowych stronom trzecim**  Dane przetwarzane w SIS oraz powiązane informacje uzupełniające podlegające wymianie na mocy niniejszego rozporządzenia nie są przekazywane ani udostępniane państwom trzecim ani organizacjom międzynarodowym. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości. |
|  | **Art. 66** | Artykuł 66  **Mające zastosowanie przepisy**  1. Rozporządzenie (UE) 2018/ 1725 stosuje się do przetwarzania danych osobowych przez eu-LISA, Europejską Agencję Straży Granicznej i Przybrzeżnej i Eurojust na mocy niniejszego rozporządzenia. Do przetwarzania danych osobowych przez Europol na mocy niniejszego rozporządzenia zastosowanie ma rozporządzenie (UE) 2016/794.  2. Do przetwarzania danych osobowych na mocy niniejszego rozporządzenia przez właściwe organy oraz służby krajowe do celów zapobiegania przestępstwom, wykrywania ich, prowadzenia w ich sprawie postępowań przygotowawczych, ścigania ich lub wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, zastosowanie ma dyrektywa (UE) 2016/680.  3. Do przetwarzania danych osobowych na mocy niniejszego rozporządzenia przez właściwe organy oraz służby krajowe zastosowanie ma rozporządzenie (UE) 2016/679, z wyjątkiem przetwarzania do celów zapobiegania przestępstwom, wykrywania ich, prowadzenia w ich sprawie postępowań przygotowawczych, ścigania ich lub wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, w którym to przypadku zastosowanie ma dyrektywa (UE) 2016/680. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości.  W zakresie art. 66 ust. 2 i 3 - ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) – w tytule ww. ustawy dodano odnośnik nr 1 w brzmieniu: Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89). |
|  | **Art. 67** | Artykuł 67  **Prawo do dostępu, sprostowania nieprawidłowych danych i usuwania danych przechowywanych niezgodnie z prawem**  1. Osoby, których dane dotyczą, mogą korzystać ze swoich praw przewidzianych w art. 15, 16 i 17 rozporządzenia (UE) 2016/679 oraz w art. 14 i art. 16 ust. 1 i 2 dyrektywy (UE) 2016/680.  2. Państwo członkowskie, inne niż państwo członkowskie dokonujące wpisu, może przekazać osobie, której dane dotyczą, informację o danych stanowiących jej dane osobowe, które są przetwarzane, wyłącznie w sytuacji, gdy najpierw umożliwiło państwu członkowskiemu dokonującemu wpisu zajęcie w tej sprawie stanowiska. Komunikacja pomiędzy państwami członkowskimi odbywa się w takich przypadkach w drodze wymiany informacji uzupełniających.  3. Państwo członkowskie podejmuje decyzję o nieprzekazywaniu całości lub części informacji osobie, której dane dotyczą, zgodnie z prawem krajowym, w zakresie – a także przez tak długi okres – w jakim takie częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów osoby, której dane dotyczą, po to aby: a) uniemożliwić utrudnianie prowadzenia urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur; b) uniemożliwić utrudnianie zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar; 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/95 c) chronić bezpieczeństwo publiczne; d) chronić bezpieczeństwo narodowe; lub e) chronić prawa i wolności innych osób. W przypadkach, o których mowa w akapicie pierwszym państwo członkowskie bez zbędnej zwłoki informuje na piśmie osobę, której dane dotyczą, o odmowie lub ograniczeniu dostępu oraz o powodach takiej odmowy lub takiego ograniczenia. Informacje takie można pominąć, jeżeli ich przekazanie godziłoby w którykolwiek z celów określonych w lit. a)-e) akapitu pierwszego. Państwo członkowskie informuje osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub możliwości skorzystania ze środka ochrony prawnej przed sądem. Państwo członkowskie dokumentuje faktyczne lub prawne powody swojej decyzji o nieinformowaniu osoby, której dane dotyczą. Informacje te udostępnia się organom nadzorczym. W takich przypadkach osoba, której dane dotyczą, może również wykonywać swoje prawa za pośrednictwem właściwych organów nadzorczych.  4. Po złożeniu wniosku o dostęp, sprostowanie lub usunięcie osoba, której dane dotyczą, jest informowana przez państwo członkowskie jak najszybciej, a w każdym razie nie później niż w terminach, o których mowa w art. 12 ust. 3 rozporządzenia (UE) 2016/679, o działaniach podjętych w związku ze skorzystaniem przez nią z tych praw na podstawie niniejszego artykułu | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości  W zakresie art. 67 ust. 1 - ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) – w tytule ww. ustawy dodano odnośnik nr 1 w brzmieniu: Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89). |
|  | **Art. 68** | Artykuł 68  **Środki ochrony prawnej**  1. Bez uszczerbku dla przepisów dotyczących środków ochrony prawnej zawartych w rozporządzeniu (UE) 2016/679 i dyrektywie (UE) 2016/680 każdej osobie przysługuje prawo do wniesienia do właściwego organu, w tym sądu, na mocy prawa krajowego państwa członkowskiego żądania o dostęp do informacji, ich sprostowanie, ich usunięcie lub ich uzyskanie lub o zapłatę odszkodowania w związku z wpisem dotyczącym tej osoby.  2. Państwa członkowskie zobowiązują się wzajemnie do wykonywania orzeczeń lub decyzji kończących postępowanie w sprawie wydanych przez sądy lub organy, o których mowa w ust. 1 niniejszego artykułu, bez uszczerbku dla art. 72.  3. Państwa członkowskie raz w roku składają Europejskiej Radzie Ochrony Danych sprawozdanie na temat: a) liczby wniosków o uzyskanie dostępu przekazanych administratorowi danych oraz liczby przypadków, w których przyznano dostęp do danych; b) liczby wniosków o uzyskanie dostępu przekazanych organowi nadzorczemu oraz liczby przypadków, w których przyznano dostęp do danych; c) liczby wniosków o sprostowanie nieprawidłowych danych oraz o usunięcie danych przechowywanych niezgodnie z prawem przekazanych administratorowi danych oraz liczby przypadków, w których dane zostały sprostowane lub usunięte; d) liczby przekazanych organowi nadzorczemu wniosków o sprostowanie nieprawidłowych danych oraz o usunięcie danych przechowywanych niezgodnie z prawem; e) liczby wszczętych postępowań sądowych; f) liczby spraw, w których sąd orzekł na korzyść strony skarżącej; g) uwag dotyczących przypadków wzajemnego uznawania orzeczeń lub decyzji kończących postępowanie w sprawie wydanych przez sądy lub organy innych państw członkowskich w odniesieniu do wpisów wprowadzonych przez państwo członkowskie dokonujące wpisu. Komisja opracuje szablon sprawozdania, o którym mowa w niniejszym ustępie.  4. Sprawozdania państw członkowskich są włączane do wspólnego sprawozdania, o którym mowa w art. 71 ust. 4. | **N** |  |  | Przepis stosowany bezpośrednio – dotyczy funkcjonowania systemu jako całości.  Zgodnie z art. 10 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym administratorem danych osobowych przetwarzanych poprzez Krajowy System Informatyczny (KSI) jest centralny organ techniczny KSI.  W myśl art. 37 ust. 1 lit. a) i ust. 7 rozporządzenia (UE) 2016/679 oraz art. 8 w zw. z jego art. 9 pkt 1, art. 10 ust. 1 i 3 i art. 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), jak również art. 46 ust. 1, 9 i 11 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), administrator wyznacza inspektora ochrony danych, udostępnia jego dane kontaktowe na swojej stronie internetowej i zawiadamia o tym organ nadzorczy – co służy zabezpieczeniu interesu osób, których przetwarzane dane dotyczą w celu umożliwienia realizacji przewidzianych w tym zakresie uprawnień.  W zakresie art. 68 ust. 1 – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) – rozdział 10. |
|  | **Art. 69** | Artykuł 69  **Nadzór nad N.SIS**  1. Państwo członkowskie zapewnia, by niezależne organy nadzorcze wyznaczone w każdym państwie członkowskim, którym to organom powierzono uprawnienia określone w rozdziale VI rozporządzenia (UE) 2016/679 lub w rozdziale VI dyrektywy (UE) 2016/680, monitorowały zgodność z prawem przetwarzania danych osobowych w SIS na ich terytorium, przekazywania tych danych z ich terytorium oraz wymiany i dalszego przetwarzania informacji uzupełniających na ich terytorium.  2. Organy nadzorcze zapewniają, by co najmniej co cztery lata przeprowadzany był audyt operacji przetwarzania danych w ramach ich N.SIS zgodnie z międzynarodowymi standardami audytu. Audyt jest prowadzony przez organy nadzorcze albo organy nadzorcze bezpośrednio zlecają przeprowadzenie audytu niezależnemu audytorowi ds. ochrony danych. Organy nadzorcze zawsze zachowują kontrolę nad niezależnym audytorem i pełnią obowiązki niezależnego audytora. L 312/96 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018  3. Państwa członkowskie zapewniają, by organy nadzorcze dysponowały zasobami wystarczającymi do wykonywania zadań powierzonych im na mocy niniejszego rozporządzenia oraz miały dostęp do doradztwa świadczonego przez osoby posiadające wystarczającą wiedzę w zakresie danych biometrycznych. | **N** |  |  | W zakresie art. 69 ust. 1 – zgodnie z art. 51 ust. 1 rozporządzenia (UE) 2016/679, każde państwo członkowskie zapewnia, by za monitorowanie stosowania RODO odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii; analogicznie, według art. 41 ust. 1 i 3 dyrektywy (UE) 2016/680, państwo członkowskie zapewnia, by za monitorowanie stosowania niniejszej dyrektywy odpowiadał co najmniej jeden niezależny organ publiczny, dla ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii – przy czym ww. organem może być organ nadzorczy ustanowiony na mocy rozporządzenia (UE) 2016/679.  W myśl art. 34 ust. 1 i 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) – Prezes Urzędu Ochrony Danych Osobowych jest w Polsce organem właściwym w sprawie ochrony danych osobowych oraz organem nadzorczym w rozumieniu rozporządzenia (UE) 2016/679 oraz w rozumieniu dyrektywy (UE) 2016/680. |
|  | **Art. 70** | Artykuł 70  **Nadzór nad eu-LISA**  1. Europejski Inspektor Ochrony Danych odpowiada za monitorowanie przetwarzania danych osobowych przez euLISA oraz za zapewnienie, by było ono prowadzone zgodnie z niniejszym rozporządzeniem. Zastosowanie mają odpowiednio zadania i uprawnienia, o których mowa w art. 57 i 58 rozporządzenia (UE) 2018/1725.  2. Europejski Inspektor Ochrony Danych co najmniej co cztery lata przeprowadza audyt w zakresie przetwarzania danych osobowych przez eu-LISA zgodny z międzynarodowymi standardami audytu. Sprawozdanie z tego audytu przesyłane jest Parlamentowi Europejskiemu, Radzie, eu-LISA, Komisji i organom nadzorczym. eu-LISA umożliwia się przedstawienie uwag przed przyjęciem sprawozdania. | **N** |  |  | Dotyczy Agencji eu-LISA. |
|  | **Art. 71** | Artykuł 71  **Współpraca krajowych organów nadzorczych i Europejskiego Inspektora Ochrony Danych**  1. Organy nadzorcze i Europejski Inspektor Ochrony Danych, działając w ramach swoich odpowiednich kompetencji, współpracują aktywnie w zakresie swoich zadań i zapewniają skoordynowany nadzór nad SIS.  2. Organy nadzorcze i Europejski Inspektor Ochrony Danych w zależności od potrzeb i w ramach swoich odpowiednich kompetencji przeprowadzają wymianę stosownych informacji, wspomagają się wzajemnie w przeprowadzaniu audytów i inspekcji, analizują trudności w zakresie wykładni lub stosowania niniejszego rozporządzenia i innych mających zastosowanie unijnych aktów prawnych, badają problemy, które wykryto w wyniku sprawowania niezależnego nadzoru lub wykonywania praw przez osoby, których dane dotyczą, sporządzają uzgodnione propozycje wspólnych rozwiązań problemów oraz upowszechniają wiedzę o prawach w zakresie ochrony danych.  3. Do celów określonych w ust. 2 organy nadzorcze i Europejski Inspektor Ochrony Danych spotykają się co najmniej dwa razy w roku w ramach Europejskiej Rady Ochrony Danych. Za koszty i obsługę tych posiedzeń odpowiada Europejska Rada Ochrony Danych. Podczas pierwszego posiedzenia zostanie przyjęty regulamin wewnętrzny. Dalsze metody pracy opracowuje się wspólnie stosownie do potrzeb.  4. Wspólne sprawozdanie z działalności dotyczącej skoordynowanego nadzoru przesyłane jest co roku przez Europejską Radę Ochrony Danych Parlamentowi Europejskiemu, Radzie i Komisji. | **N** |  |  | Dotyczy współpracy Prezesa Urzędu Ochrony Danych Osobowych i Europejskiego Inspektora Ochrony Danych. |
|  | **Art. 72** | Artykuł 72  **Odpowiedzialność**  1. Bez uszczerbku dla prawa do odszkodowania oraz odpowiedzialności na mocy rozporządzenia (UE) 2016/679, dyrektywy (UE) 2016/680 i rozporządzenia (UE) 2018/1725: a) osoba lub państwo członkowskie, które poniosły szkodę majątkową lub niemajątkową w wyniku niezgodnej z prawem operacji przetwarzania danych osobowych w związku z użytkowaniem N.SIS lub innego działania niezgodnego z niniejszym rozporządzeniem przeprowadzonych przez jedno z państw członkowskich, są uprawnione do odszkodowania od tego państwa członkowskiego; oraz b) osoba lub państwo członkowskie, które poniosły szkodę majątkową lub niemajątkową w wyniku działania eu-LISA niezgodnego z niniejszym rozporządzeniem, są uprawnione do otrzymania odszkodowania od eu-LISA. Państwo członkowskie lub eu-LISA zostają zwolnione z odpowiedzialności na podstawie akapitu pierwszego, w całości lub w części, jeżeli wykażą, że nie ponoszą odpowiedzialności za zdarzenie, które spowodowało szkodę. 2. Jeżeli niewypełnienie przez państwo członkowskie obowiązków spoczywających na nim zgodnie z niniejszym rozporządzeniem spowoduje szkodę w SIS, wówczas to państwo członkowskie ponosi odpowiedzialność za tę szkodę, chyba że – i w zakresie w jakim – eu-LISA lub inne państwo członkowskie uczestniczące w SIS nie podjęły rozsądnych środków, by zapobiec wystąpieniu szkody lub zminimalizować jej skutki.  3. Kwestie związane z roszczeniami o odszkodowanie wnoszonymi przeciwko państwu członkowskiemu z tytułu szkody, o której mowa w ust. 1 i 2, regulują przepisy prawa krajowego tego państwa członkowskiego. Roszczenia o odszkodowanie wnoszone przeciwko eu-LISA z tytułu szkody, o której mowa w ust. 1 i 2, podlegają warunkom przewidzianym w Traktatach. | **N** |  |  | Przepisy ogólne o skutku bezpośrednim dotyczące wszystkich podmiotów. |
|  | **Art. 73** | Artykuł 73  **Sankcje**  Państwa członkowskie zapewniają, aby wszelkie przypadki niezgodnego z niniejszym rozporządzeniem wykorzystania danych SIS, przetwarzania takich danych lub wymiany informacji uzupełniających podlegały sankcjom zgodnie z prawem krajowym. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. | **N** |  |  | Przepisy ogólne o skutku bezpośrednim dotyczące wszystkich podmiotów. |
|  | **Art. 74** | Artykuł 74  **Monitorowanie i statystyki**  1. eu-LISA zapewnia, by istniały procedury pozwalające monitorować, czy SIS działa zgodnie z wyznaczonymi celami, w tym w odniesieniu do wyników, opłacalności, bezpieczeństwa i jakości usług.  2. Na użytek prac konserwacyjno-technicznych, przygotowywania sprawozdań, sprawozdawczości na temat jakości danych i sporządzania statystyk eu-LISA ma dostęp do niezbędnych informacji związanych z operacjami przetwarzania danych wykonywanymi w systemie centralnym SIS.  3. eu-LISA sporządza dzienne, miesięczne i roczne statystyki pokazujące liczbę rekordów przypadających na daną kategorię wpisów, zarówno w odniesieniu do poszczególnych państw członkowskich, jak i w ujęciu zagregowanym. euLISA sporządza również roczne sprawozdania na temat liczby uzyskanych w systemie trafień przypadających na daną kategorię wpisów, liczby wyszukiwań w SIS oraz liczby przypadków skorzystania z dostępu do SIS w celu wprowadzenia, zaktualizowania lub usunięcia wpisu, zarówno w odniesieniu do poszczególnych państw członkowskich, jak i w ujęciu zagregowanym. Sporządzane statystyki nie zawierają żadnych danych osobowych. Roczne sprawozdanie statystyczne podlega publikacji.  4. Państwa członkowskie, Europol, Eurojust i Europejska Agencja Straży Granicznej i Przybrzeżnej przekazują euLISA i Komisji informacje niezbędne do sporządzenia sprawozdań, o których mowa w ust. 3, 6, 8 i 9.  5. Informacje te obejmują odrębne statystyki dotyczące liczby wyszukiwań przeprowadzonych przez służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych pojazdów oraz służby państw członkowskich odpowiedzialne za wydawanie dowodów rejestracyjnych jednostek pływających lub za zarządzanie ruchem takich jednostek, w tym w odniesieniu do silników jednostek pływających, oraz statków powietrznych, w tym silników statków powietrznych, oraz broni palnej, lub w imieniu tych służb. Statystyki te pokazują również liczbę trafień przypadających na daną kategorię wpisów.  6. eu-LISA przekazuje Parlamentowi Europejskiemu, Radzie, państwom członkowskim, Komisji, Europolowi, Eurojustowi, Europejskiej Agencji Straży Granicznej i Przybrzeżnej oraz Europejskiemu Inspektorowi Ochrony Danych sporządzone przez siebie sprawozdania statystyczne. Aby móc monitorować wdrażanie unijnych aktów prawnych, w tym do celów rozporządzenia (UE) nr 1053/2013, Komisja może zwrócić się do eu-LISA o regularne lub doraźne sporządzanie dodatkowych szczególnych sprawozdań statystycznych dotyczących działania SIS, użytkowania SIS i wymiany informacji uzupełniających. Europejska Agencja Straży Granicznej i Przybrzeżnej może zwrócić się do eu-LISA o regularne lub doraźne sporządzanie dodatkowych szczególnych sprawozdań statystycznych do celów przeprowadzania analiz ryzyka i ocen narażenia, o których mowa w rozporządzeniu (UE) 2016/1624.  7. Na użytek art. 15 ust. 4 oraz ust. 3, 4 i 6 niniejszego artykułu eu-LISA ustanawia, wdraża i obsługuje w swoich centrach technicznych centralne repozytorium zawierające dane, o których mowa w art. 15 ust. 4 oraz w ust. 3 niniejszego artykułu, które nie umożliwią identyfikacji poszczególnych osób, ale umożliwią Komisji oraz agencjom wymienionym w ust. 6 niniejszego artykułu uzyskanie dostosowanych do ich potrzeb sprawozdań i statystyk. Na wniosek eu-LISA udziela państwom członkowskim, Komisji, Europolowi, Eurojustowi i Europejskiej Agencji Straży Granicznej i Przybrzeżnej – w zakresie, w jakim jest to niezbędne do wykonywania ich zadań – dostępu do centralnego repozytorium w drodze bezpiecznego dostępu za pośrednictwem infrastruktury łączności. eu-LISA wprowadza kontrole dostępu i specjalne profile użytkownika, aby dostęp do centralnego repozytorium był wykorzystywany wyłącznie do sporządzania sprawozdań i statystyk.  8. Dwa lata po dacie rozpoczęcia stosowania niniejszego rozporządzenia zgodnie z art. 79 ust. 5 akapit pierwszy, a następnie co dwa lata eu-LISA przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie na temat technicznych aspektów funkcjonowania systemu centralnego SIS i infrastruktury łączności, w tym kwestii ich bezpieczeństwa, Automatycznego Systemu Identyfikacji Daktyloskopijnej oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi. Sprawozdanie to zawiera również ocenę wykorzystywania wizerunków twarzy do identyfikowania osób, po tym jak technologia ta zostanie wprowadzona do użytku. L 312/98 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 9. Trzy lata po dacie rozpoczęcia stosowania niniejszego rozporządzenia zgodnie z art. 79 ust. 5 akapit pierwszy, a następnie co cztery lata Komisja przeprowadza ogólną ocenę systemu centralnego SIS oraz dwustronnej i wielostronnej wymiany informacji uzupełniających pomiędzy państwami członkowskimi. W tej ogólnej ocenie zawiera się analizę osiągniętych wyników w zestawieniu z celami i ocenia się, na ile wciąż aktualne są pierwotne przesłanki, w jaki sposób niniejsze rozporządzenie stosowane jest do systemu centralnego SIS, na ile bezpieczny jest system centralny SIS i jakie będą konsekwencje dla przyszłych operacji. Sprawozdanie z oceny zawiera także ocenę Automatycznego Systemu Identyfikacji Daktyloskopijnej oraz kampanii informacyjnych na temat SIS przeprowadzonych przez Komisję zgodnie z art. 19. Komisja przekazuje sprawozdanie z oceny Parlamentowi Europejskiemu i Radzie.  10. Komisja przyjmuje akty wykonawcze w celu określenia szczegółowych zasad dotyczących funkcjonowania centralnego repozytorium, o którym mowa w ust. 7 niniejszego artykułu, oraz zasad ochrony danych i zasad bezpieczeństwa mających zastosowanie do tego repozytorium. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 76 ust. 2. | **N** |  |  | Dotyczy Agencji eu-LISA. |
|  | **Art. 75** | Artykuł 75  **Wykonywanie przekazanych uprawnień**  1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.  2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 38 ust. 3 i w art. 43 ust. 4, powierza się Komisji na czas nieokreślony od dnia 27 grudnia 2018 r.  3. Przekazanie uprawnień, o którym mowa w art. 38 ust. 3 i w art. 43 ust. 4, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.  4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.  5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.  6. Akt delegowany przyjęty na podstawie art. 38 ust. 3 lub art. 43 ust. 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady. | **N** |  |  | Dotyczy zadań Komisji Europejskiej. |
|  | **Art. 76** | Artykuł 76  **Procedura komitetowa**  1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.  2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011. | **N** |  |  | Dotyczy procedury komitetowej. |
|  | **Art. 77** | Artykuł 77  **Zmiany w decyzji 2007/533/WSiSW**  W decyzji 2007/533/WSiSW wprowadza się następujące zmiany: 1) art. 6 otrzymuje brzmienie: „Artykuł 6 Systemy krajowe 1. Każde państwo członkowskie odpowiada za utworzenie, funkcjonowanie, utrzymanie i dalsze rozwijanie własnego N.SIS II oraz za przyłączenie go do NI-SIS. 2. Każde państwo członkowskie odpowiada za zapewnienie użytkownikom końcowym niezakłóconej dostępności danych SIS II.”; 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/99 2) art. 11 otrzymuje brzmienie: „Artykuł 11 Poufność – państwa członkowskie 1. Każde państwo członkowskie stosuje, zgodnie ze swoim prawem krajowym, swoje przepisy dotyczące tajemnicy zawodowej lub inne równoważne wymogi poufności wobec wszystkich osób i podmiotów, które muszą operować danymi SIS II i informacjami uzupełniającymi. Zobowiązanie to obowiązuje także po zakończeniu pełnienia urzędu lub ustaniu zatrudnienia oraz po zakończeniu działalności przez dane podmioty. 2. W przypadku gdy dane państwo członkowskie współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS II, ściśle monitoruje ono działania wykonawcy, by zapewnić przestrzeganie wszelkich przepisów niniejszej decyzji, w szczególności dotyczących bezpieczeństwa, poufności i ochrony danych. 3. Zarządzania operacyjnego N.SIS II lub kopiami technicznymi nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym.”; 3) w art. 15 wprowadza się następujące zmiany: a) dodaje się ustęp w brzmieniu: „3a. Organ zarządzający opracowuje i utrzymuje mechanizm i procedury do celów przeprowadzania kontroli jakości danych w CS-SIS. Przekazuje on państwom członkowskim regularne sprawozdania na ten temat. Organ zarządzający przekazuje Komisji regularne sprawozdania, w których uwzględnia napotkane problemy i państwa członkowskie, których problemy te dotyczą. Komisja przekazuje Parlamentowi Europejskiemu i Radzie regularne sprawozdania na temat napotkanych problemów związanych z jakością danych.”; b) ust. 8 otrzymuje brzmienie: „8. Zarządzanie operacyjne centralnym SIS II obejmuje wszystkie zadania niezbędne do tego, by centralny SIS II działał zgodnie z niniejszą decyzją przez 24 godziny na dobę, 7 dni w tygodniu – w szczególności prace konserwacyjne oraz udoskonalenia techniczne niezbędne do sprawnego działania systemu. Zadania te obejmują również koordynowanie działań w zakresie testowania, zarządzanie tymi działaniami i ich wspieranie w odniesieniu do centralnego SIS II i N.SIS II, zapewniające funkcjonowanie centralnego SIS II i N.SIS zgodnie z wymogami zgodności pod względem technicznym określonymi w art. 9”; 4) w art. 17 dodaje się ustępy w brzmieniu: „3. W przypadku gdy organ zarządzający współpracuje z wykonawcami zewnętrznymi przy zadaniach związanych z SIS II, organ ten ściśle monitoruje działania wykonawcy, by zapewnić przestrzeganie wszystkich przepisów niniejszej decyzji, w szczególności dotyczących bezpieczeństwa, poufności i ochrony danych. 4. Zarządzania operacyjnego CS-SIS nie powierza się przedsiębiorstwom prywatnym ani organizacjom prywatnym.”; 5) w art. 21 dodaje się akapit w brzmieniu: „Jeżeli dana osoba lub dany przedmiot są poszukiwane na podstawie wpisu dotyczącego przestępstwa terrorystycznego, dany przypadek uznaje się za wystarczająco adekwatny, odpowiedni i ważny, by uzasadniać wpis w SIS II. Ze względu na bezpieczeństwo publiczne lub narodowe państwa członkowskie mogą wyjątkowo nie wprowadzać wpisu, jeśli istnieje prawdopodobieństwo, że utrudniłby on prowadzenie dochodzeń urzędowych lub sądowych, postępowań przygotowawczych lub innych postępowań.”; 6) art. 22 otrzymuje brzmienie: „Artykuł 22 Przepisy szczegółowe dotyczące wprowadzania, weryfikacji lub wyszukiwania przy użyciu fotografii i odbitek linii papilarnych palców 1. Fotografie i odciski palców wprowadza się wyłącznie po przeprowadzeniu specjalnej kontroli jakości służącej stwierdzeniu, czy spełniają one minimalne normy jakości danych. Specyfikacja tej specjalnej kontroli jakości jest określana zgodnie z procedurą, o której mowa w art. 67. 2. Jeżeli fotografie i odbitki linii papilarnych palców są dostępne we wpisie w SIS II, takie fotografie i odbitki linii papilarnych palców wykorzystuje się do potwierdzenia tożsamości osoby, która została zlokalizowana w wyniku wyszukiwania alfanumerycznego przeprowadzonego w SIS II. 3. Wyszukiwanie przy użyciu odbitek linii papilarnych palców może być przeprowadzone we wszystkich przypadkach w celu identyfikacji danej osoby. Jednakże jeżeli tożsamości danej osoby nie można ustalić w żaden inny sposób, w celu identyfikacji przeprowadza się wyszukiwanie przy użyciu odbitek linii papilarnych palców. W tym celu centralny SIS II posiada Automatyczny System Identyfikacji Daktyloskopijnej. L 312/100 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 4. Odbitki linii papilarnych palców w SIS II związane z wpisami wprowadzonymi zgodnie z art. 26, 32 i 36 można wyszukiwać również przy użyciu kompletnych lub niekompletnych zestawów odbitek linii papilarnych palców, które znaleziono na miejscu popełnienia poważnych przestępstw lub przestępstw terrorystycznych będących przedmiotem postępowania przygotowawczego, w przypadku których z dużym prawdopodobieństwem można stwierdzić, że te zestawy odbitek linii papilarnych palców należą do sprawcy danego przestępstwa oraz pod warunkiem że wyszukiwanie przeprowadzane jest równolegle w odpowiednich bazach danych państw członkowskich zawierających odbitki linii papilarnych palców.”; 7) art. 41 otrzymuje brzmienie: „Artykuł 41 Dostęp Europolu do danych w SIS II 1. Jeżeli jest to niezbędne do wykonywania jej mandatu, Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794 (\*), ma prawo do dostępu do danych w SIS II i do przeprowadzania ich wyszukiwania. Europol może także dokonywać wymiany informacji uzupełniających i występować z wnioskami o dalsze informacje uzupełniające zgodnie z zasadami zawartymi w podręczniku SIRENE. 2. Jeżeli podczas wyszukiwania Europol stwierdzi istnienie wpisu w SIS II, informuje o tym – w drodze wymiany informacji uzupełniających przy użyciu infrastruktury łączności i zgodnie z zasadami zawartymi w podręczniku SIRENE – państwo członkowskie dokonujące wpisu. Dopóki Europol nie będzie w stanie korzystać z funkcji przewidzianych do wymiany informacji uzupełniających, w celu przekazywania informacji państwom członkowskim dokonującym wpisu wykorzystuje kanały określone w rozporządzeniu (UE) 2016/794. 3. Europol może przetwarzać informacje uzupełniające, które przekazały mu państwa członkowskie, do celów przeprowadzania porównania ich ze swoimi bazami danych i projektami analitycznymi, mającego służyć wskazaniu powiązań lub innych odpowiednich związków, oraz do celów analiz strategicznych, tematycznych lub operacyjnych, o których mowa w art. 18 ust. 2 lit. a), b) i c) rozporządzenia (UE) 2016/794. Europol przetwarza informacje uzupełniające do celów niniejszego artykułu zgodnie z tym rozporządzeniem. 4. Wykorzystanie przez Europol informacji uzyskanych w wyniku wyszukiwania w SIS II lub w wyniku przetwarzania informacji uzupełniających wymaga zgody państwa członkowskiego dokonującego wpisu. Jeżeli to państwo członkowskie zezwoli na wykorzystanie takich informacji, posługiwanie się nimi przez Europol regulowane jest rozporządzeniem (UE) 2016/794. Europol przekazuje takie informacje państwom trzecim i podmiotom trzecim wyłącznie za zgodą państwa członkowskiego dokonującego wpisu i z pełnym poszanowaniem prawa Unii dotyczącego ochrony danych. 5. Europol: a) bez uszczerbku dla ust. 4 i 6 nie podłącza części SIS II ani nie przekazuje zawartych w nich danych, do których ma dostęp, do systemu gromadzenia i przetwarzania danych stosowanego przez Europol lub w Europolu, a także nie pobiera ani w inny sposób nie kopiuje żadnych części SIS II; b) niezależnie od art. 31 ust. 1 rozporządzenia (UE) 2016/794 usuwa informacje uzupełniające zawierające dane osobowe najpóźniej rok po usunięciu związanego z nimi wpisu. Na zasadzie odstępstwa, jeżeli Europol posiada w swoich bazach danych lub projektach analitycznych informacje o sprawie, której dotyczą informacje uzupełniające, w celu wykonywania swoich zadań Europol może wyjątkowo w razie potrzeby nadal przechowywać te informacje uzupełniające. Europol informuje państwo członkowskie dokonujące wpisu i wykonujące państwo członkowskie o dalszym przechowywaniu takich informacji uzupełniających i przedstawia uzasadnienie takiego postępowania; c) ogranicza dostęp do danych w SIS II, w tym do informacji uzupełniających, tak by korzystali z niego tylko specjalnie uprawnieni pracownicy Europolu, którym dostęp do takich danych jest potrzebny do wykonywania ich zadań; d) przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13; e) zapewnia, by pracownicy uprawnieni do przetwarzania danych SIS II przeszli odpowiednie szkolenie i zostali odpowiednio poinformowani zgodnie z art. 14; oraz f) bez uszczerbku dla rozporządzenia (UE) 2016/794 zapewnia Europejskiemu Inspektorowi Ochrony Danych możliwość monitorowania i kontrolowania działań podejmowanych przez Europol w ramach wykonywania prawa do dostępu do danych w SIS II i ich wyszukiwania oraz w ramach wymiany i przetwarzania informacji uzupełniających. 6. Europol kopiuje dane z SIS II wyłącznie do celów technicznych, jeżeli takie kopiowanie jest niezbędne do przeprowadzenia bezpośredniego wyszukiwania przez należycie uprawnionych pracowników Europolu. Do takich kopii zastosowanie ma niniejsza decyzja. Kopię techniczną wykorzystuje się wyłącznie do przechowywania danych SIS II w trakcie przeprowadzania ich wyszukiwania. Po przeprowadzeniu wyszukiwania danych dane te są usuwane. Takich przypadków wykorzystywania danych nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie danych SIS II. Europol nie kopiuje do innych systemów Europolu danych zawartych we wpisach ani danych dodatkowych wprowadzonych przez państwa członkowskie lub pochodzących z CS-SIS II. 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/101 7. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europol rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS II oraz każde wyszukiwanie w SIS II. Prowadzenia takiej rejestracji i dokumentacji nie uznaje się za niezgodne z prawem pobieranie lub kopiowanie części SIS II. 8. Państwa członkowskie informują Europol w drodze wymiany informacji uzupełniających o każdym trafieniu odnoszącym się do wpisów dotyczących przestępstw terrorystycznych. Państwa członkowskie mogą w wyjątkowych okolicznościach nie przekazywać Europolowi takich informacji, jeżeli takie przekazanie mogłoby spowodować zagrożenie dla realizowanych czynności lub bezpieczeństwa osób lub byłoby sprzeczne z istotnymi interesami w zakresie bezpieczeństwa państwa członkowskiego dokonującego wpisu. 9. Ust. 8 stosuje się od daty, z którą Europol będzie w stanie otrzymywać informacje uzupełniające zgodnie z ust. 1. (\*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).”; 8) dodaje się artykuł w brzmieniu: „Artykuł 42a Dostęp zespołów Europejskiej Straży Granicznej i Przybrzeżnej, zespołów składających się z personelu realizującego zadania w dziedzinie powrotów oraz członków zespołów wspierających zarządzanie migracjami do danych w SIS II 1. Zgodnie z art. 40 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1624 (\*) członkowie zespołów, o których mowa w art. 2 pkt 8 i 9 tego rozporządzenia, mają – w ramach swojego mandatu oraz pod warunkiem że są uprawnieni do przeprowadzania kontroli zgodnie z art. 40 ust. 1 niniejszej decyzji i przeszli wymagane szkolenie zgodnie z art. 14 niniejszej decyzji – prawo do dostępu do danych w SIS II oraz do wyszukiwania takich danych w zakresie, w jakim jest to niezbędne do wykonywania ich zadań i zgodnie z wymogami planu operacyjnego dla danej operacji. Pozostali członkowie zespołów nie są uprawnieni do dostępu do danych w SIS II. 2. Członkowie zespołów, o których mowa w ust. 1, wykonują prawo do dostępu do danych w SIS II oraz do wyszukiwania takich danych zgodnie z ust. 1, korzystając z interfejsu technicznego. Interfejs techniczny zostanie utworzony i będzie prowadzony przez Europejską Agencję Straży Granicznej i Przybrzeżnej i będzie umożliwiał bezpośrednie połączenie z centralnym SIS II. 3. Jeżeli w wyniku wyszukiwania członek zespołów, o których mowa w ust. 1 niniejszego artykułu, stwierdzi istnienie wpisu w SIS II, powiadamia się o tym fakcie państwo członkowskie dokonujące wpisu. Zgodnie z art. 40 rozporządzenia (UE) 2016/1624 członkowie zespołów podejmują działania w odpowiedzi na wpis w SIS II wyłącznie na polecenie i – co do zasady – w obecności funkcjonariuszy straży granicznej lub personelu realizującego zadania w dziedzinie powrotów z przyjmującego państwa członkowskiego, w którym działają. Przyjmujące państwo członkowskie może upoważnić członków zespołów do działania w jego imieniu. 4. Do celów weryfikacji zgodności przetwarzania danych z prawem, monitorowania własnej działalności oraz zapewniania należytego bezpieczeństwa i integralności danych Europejska Agencja Straży Granicznej i Przybrzeżnej rejestruje zgodnie z przepisami art. 12 każdy dostęp do SIS II oraz każde wyszukiwanie w SIS II. 5. Europejska Agencja Straży Granicznej i Przybrzeżnej przyjmuje i stosuje środki służące zapewnieniu bezpieczeństwa, poufności i monitorowania własnej działalności zgodnie z art. 10, 11 i 13 oraz zapewnia, by zespoły, o których mowa w ust. 1 niniejszego artykułu, stosowały te środki. 6. Niniejszego artykułu nie można interpretować jako mających wpływ na przepisy rozporządzenia (UE) 2016/1624 dotyczące ochrony danych i odpowiedzialności Europejskiej Agencji Straży Granicznej i Przybrzeżnej za nieuprawnione lub nieprawidłowe przetwarzanie danych. 7. Bez uszczerbku dla ust. 2 żadnych części SIS II nie podłącza się do systemu gromadzenia i przetwarzania danych stosowanego przez zespoły, o których mowa w ust. 1 lub przez Europejską Agencję Straży Granicznej i Przybrzeżnej, a danych w SIS II, do których dostęp mają te zespoły, nie przekazuje się do takiego systemu. Nie można pobierać ani kopiować żadnych części SIS II. Rejestrowania dostępu i wyszukiwania nie uznaje się za niezgodne z prawem pobierane lub kopiowanie danych SIS II. L 312/102 PL Dziennik Urzędowy Unii Europejskiej 7.12.2018 8. Europejska Agencja Straży Granicznej i Przybrzeżnej umożliwia Europejskiemu Inspektorowi Ochrony Danych monitorowanie i kontrolowanie działań prowadzonych przez zespoły, o których mowa w niniejszym artykule, w ramach wykonywania ich prawa do dostępu do SIS II i wyszukiwania danych w SIS II. Pozostaje to bez uszczerbku dla dalszych przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (\*\*). (\*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 i uchylające rozporządzenie (WE) nr 863/2007 Parlamentu Europejskiego i Rady, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE (Dz.U. L 251 z 16.9.2016, s. 1). (\*\*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).”. | **N** |  |  | Konieczność zachowania spójności brzmienia decyzji 2007/533/WSiSW z niniejszym rozporządzeniem. |
|  | **Art. 78** | Artykuł 78  **Uchylenie**  Rozporządzenie (WE) nr 1986/2006 oraz decyzje 2007/533/WSiSW i 2010/261/UE uchyla się z dniem rozpoczęcia stosowania niniejszego rozporządzenia, określonym w jego art. 79 ust. 5 akapit pierwszy. Odesłania do uchylonych rozporządzenia (WE) nr 1986/2006 oraz decyzji 2007/533/WSiSW traktuje się jako odesłania do niniejszego rozporządzenia, zgodnie z tabelami korelacji w załączniku. | **N** |  |  | Przepis uchylający rozporządzenie (WE) nr 1986/2006 oraz decyzje 2007/533/WSiSW i 2010/261/UE. |
|  | **Art. 79** | Artykuł 79  **Wejście w życie, rozpoczęcie eksploatacji i rozpoczęcie stosowania**  1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.  2. Nie później niż dnia 28 grudnia 2021 r. Komisja przyjmie decyzję określającą datę rozpoczęcia eksploatacji SIS zgodnie z niniejszym rozporządzeniem, po zweryfikowaniu, czy spełnione są następujące warunki: a) przyjęto akty wykonawcze niezbędne do stosowania niniejszego rozporządzenia; b) państwa członkowskie powiadomiły Komisję o zakończeniu niezbędnych technicznych i prawnych przygotowań do przetwarzania danych SIS i wymiany informacji uzupełniających zgodnie z niniejszym rozporządzeniem; oraz c) eu-LISA powiadomiła Komisję o pomyślnym zakończeniu wszystkich działań w zakresie testowania w odniesieniu do CS-SIS i interakcji między CS-SIS i N.SIS.  3. Komisja monitoruje proces stopniowego spełniania warunków określonych w ust. 2 oraz informuje Parlament Europejski i Radę o wynikach weryfikacji, o której mowa w tym ustępie.  4. Do dnia 28 grudnia 2019 r., a następnie co roku do czasu przyjęcia przez Komisję decyzji, o której mowa w ust. 2, Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie o stanie przygotowań do pełnego wdrożenia niniejszego rozporządzenia. Sprawozdanie zawiera także szczegółowe informacje o poniesionych kosztach oraz informacje dotyczące wszelkich rodzajów ryzyka, które mogą mieć wpływ na ogólne koszty.  5. Niniejsze rozporządzenie stosuje się od daty określonej zgodnie z ust. 2. Na zasadzie odstępstwa od akapitu pierwszego: a) art. 4 ust. 4, art. 5, art. 8 ust. 4, art. 9 ust. 1 i 5, art. 12 ust. 8, art. 15 ust. 7, art. 19, art. 20 ust. 4 i 5, art. 26 ust. 6, art. 32 ust. 9, art. 34 ust. 3, art. 36 ust. 6, art. 38 ust. 3 i 4, art. 42 ust. 5, art. 43 ust. 4, art. 54 ust. 5, art. 62 ust. 4, art. 63 ust. 6, art. 74 ust. 7 i 10, art. 75, art. 76, art. 77 pkt 1–5 oraz ust. 3 i 4 niniejszego artykułu stosuje się od daty wejścia w życie niniejszego rozporządzenia; 7.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 312/103 b) art. 77 pkt 7 i 8 stosuje się od dnia 28 grudnia 2019 r.; c) art. 77 pkt 6 stosuje się od dnia 28 grudnia 2020 r..  6. Decyzję Komisji, o której mowa w ust. 2, publikuje się w Dzienniku Urzędowym Unii Europejskiej. | **T** | Art. 3 | Art. 3. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:  1) art. 1 pkt 4 w zakresie zmienianego art. 3 ust. 1 pkt 15 oraz art. 1 pkt 5 w zakresie zmienianego art. 4 ust. 1 pkt 16, które wchodzą w życie z dniem następującym po dniu ogłoszenia;  2) art. 1 pkt 2 lit. d w zakresie zmienianego art. 2 pkt 14a i pkt 15a, art. 1 pkt 4 w zakresie zmienianego art. 3 ust. 1 pkt 1–14 i ust. 2–5, art. 1 pkt 5 w zakresie zmienianego art. 4 ust. 1 pkt 1–15 i ust. 2–9 oraz art. 1 pkt 3, 6–12, 13, 15, 16 i 19, które wchodzą w życie z dniem określonym w decyzji Komisji, zgodnie z art. 66 ust. 2 rozporządzenia 2018/1861 oraz art. 79 ust. 2 rozporządzenia 2018/1862. | Konieczność zachowania spójności terminów wejścia ustawy w życie z terminami określonymi w rozporządzeniu.  Art. 79 ust. 2, 3, 4 i 6 nie wymagają transpozycji. |