UZASADNIENIE

Projektowana ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiającego system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określającego warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniającego konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz. Urz. UE L 327 z 09.12.2017, str. 20, z późn. zm.), zwanego dalej „rozporządzeniem 2017/2226”.

Powyższe rozporządzenie ustanawia – w celu skuteczniejszego zarządzania granicami zewnętrznymi oraz w szczególności w celu weryfikacji przestrzegania przepisów dotyczących dozwolonego okresu pobytu na terytorium państw członkowskich – System Wjazdu/Wyjazdu (EES), zwany dalej „Systemem”, rejestrujący elektronicznie czas i miejsce wjazdu i wyjazdu obywateli państw trzecich dopuszczonych do pobytu krótkoterminowego na terytorium państw członkowskich oraz obliczający okres ich dozwolonego pobytu. Ma on zastąpić system obowiązkowego stemplowania paszportów obywateli państw trzecich, który stosują wszystkie państwa członkowskie. Ponadto w Systemie będą ewidencjonowane decyzje o odmowie wjazdu.

W rozporządzeniu 2017/2226 określono kategorie danych, które będą wprowadzane do EES, cele, do jakich dane będą wykorzystywane, kryteria ich wprowadzania, organy uprawnione do dostępu do danych, dalsze zasady przetwarzania danych i ochrony danych osobowych, a także architekturę techniczną EES, zasady dotyczące jego funkcjonowania i użytkowania oraz interoperacyjność z innymi systemami informacyjnymi.

Projektowana ustawa określa zasady i sposób realizacji udziału Rzeczypospolitej Polskiej w Systemie, w tym obowiązki i uprawnienia organów dotyczące przetwarzania danych zawartych w EES poprzez Krajowy System Informatyczny do spraw Systemu.

Art. 1 ustawy określa zakres projektowanej regulacji.

W projektowanym art. 2 zawarto definicje podstawowych pojęć, w tym przez odwołanie się do odpowiednich przepisów rozporządzenia 2017/2226.

W art. 3 określono podmioty uprawnione do bezpośredniego dostępu do KSI EES w celu realizacji:

1. przez organy imigracyjne uprawnienia wynikającego z art. 12 ust. 3 rozporządzenia 2017/2226, czyli możliwości generowania wykazu zawierającego dane wszystkich osób zidentyfikowanych jako osoby przekraczające okres dozwolonego pobytu, w celu podejmowania przez nie odpowiednich działań. W związku z imigracyjnym charakterem uprawnienia projekt przewiduje, że będzie ono przysługiwało Straży Granicznej, wojewodzie, Szefowi Urzędu do Spraw Cudzoziemców, konsulowi i ministrowi właściwemu do spraw zagranicznych;
2. przez służbę graniczną oraz organy imigracyjne obowiązków określonych w art. 19 rozporządzenia 2017/2226, tj. w przypadku cofnięcia, unieważnienia lub przedłużenia zezwolenia na pobyt krótkoterminowy. W związku z charakterem ww. czynności, wykonywanej podczas wykonywania czynności wobec cudzoziemców na podstawie innych przepisów, uprawnienie do dostępu do KSI EES w tym celu będzie przysługiwało ministrowi właściwemu do spraw zagranicznych, ministrowi właściwemu do spraw wewnętrznych, konsulowi, Szefowi Urzędu do Spraw Cudzoziemców, wojewodzie oraz Straży Granicznej;
3. przez służbę graniczną obowiązków określonych w art. 14 ust. 1–7 rozporządzenia 2017/2226, czyli tworzenia rejestru indywidualnego, dokonywania jego aktualizacji oraz wprowadzaniu wpisu dotyczącego wjazdu, wyjazdu lub odmowy wjazdu. W związku z granicznym charakterem obowiązku zakłada się, że uprawnienie do dostępu do KSI EES w tym celu będzie przysługiwało Straży Granicznej;
4. przez organy imigracyjne oraz wizowe obowiązku określonego w art. 14 ust. 8 rozporządzenia 2017/2226, czyli utworzenia rejestru indywidualnego i wpisu dotyczącego wjazdu/wyjazdu na wniosek obywatela państwa trzeciego przebywającego na terytorium państwa członkowskiego, którego pobyt krótkoterminowy rozpoczyna się bezpośrednio po pobycie na podstawie dokumentu pobytowego lub wizy długoterminowej i nie utworzono wcześniej rejestru indywidualnego. W związku z charakterem ww. czynności, które powodują powstanie obowiązku wykonania czynności w Systemie, uprawnienie do dostępu do KSI EES w tym celu będzie przysługiwało Straży Granicznej, wojewodzie i Szefowi Urzędu do Spraw Cudzoziemców;
5. obowiązku wynikającego z art. 20 rozporządzenia 2017/2226, tj. utworzenia rejestru indywidualnego, aktualizacji ostatniego wpisu dotyczącego wjazdu/wyjazdu oraz usuwania istniejącego rejestru w przypadku obalenia domniemania, że obywatel państwa trzeciego nie spełnia warunków związanych z okresem dozwolonego pobytu na terytorium państw członkowskich lub przestał te warunki spełniać – będzie przysługiwało Straży Granicznej, wojewodzie i Szefowi Urzędu do Spraw Cudzoziemców;
6. obowiązku wynikającego z art. 23 rozporządzenia 2017/2226, tj. zweryfikowania tożsamości i wcześniejszej rejestracji obywatela państwa trzeciego, w celu aktualizacji danych EES oraz w celu przeglądania danych w zakresie, w jakim jest to niezbędne do dokonywania odpraw granicznych. W związku z granicznym charakterem uprawnienia zostanie ono przyznane Straży Granicznej;
7. obowiązku określonego w art. 25 rozporządzenia 2017/2226, tj. przeglądania EES w celu rozpatrywania wniosków o dostęp do krajowych programów ułatwień (o których mowa w art. 8d rozporządzenia 2016/399) oraz w celu wydawania decyzji dotyczących tych wniosków. Uprawnienie będzie przysługiwać Straży Granicznej, wojewodzie, Szefowi Urzędu do Spraw Cudzoziemców, konsulowi i ministrowi właściwemu do spraw zagranicznych;
8. uprawnienia określonego w art. 26 rozporządzenia 2017/2226, tj. weryfikacji tożsamości obywatela państwa trzeciego lub sprawdzenia, lub zweryfikowania, czy spełnione zostały warunki wjazdu lub pobytu na terytorium państw członkowskich. W związku z migracyjnym charakterem uprawnienia związanym z przeprowadzaniem kontroli legalności pobytu cudzoziemców na terytorium Rzeczypospolitej Polskiej, o której mowa w art. 289 ustawy o cudzoziemcach, projekt zakłada, że uprawnienie to będzie przysługiwało Straży Granicznej, wojewodzie, Szefowi Urzędu do Spraw Cudzoziemców, Policji i Krajowej Administracji Skarbowej;
9. uprawnienia, o którym mowa w art. 27 rozporządzenia 2017/2226, tj. zidentyfikowania obywatela państwa trzeciego, który mógł zostać uprzednio zarejestrowany w EES pod inną tożsamością lub który nie spełnia warunków wjazdu lub pobytu na terytorium państw członkowskich lub przestał spełniać te warunki. W związku z graniczno-migracyjnym charakterem ww. czynności uprawnienie to będzie przysługiwać Straży Granicznej, wojewodzie, Szefowi Urzędu do Spraw Cudzoziemców, Policji i Krajowej Administracji Skarbowej.

Projektowana ustawa zobowiązuje organy wprowadzające dane do Systemu do zapewnienia wysokiej jakości danych, rozumianej jako ich zgodność z prawem, dokładność i aktualność, do czego zobowiązuje państwa członkowskie art. 39 rozporządzenia 2017/2226. Ponadto, w razie potrzeby, dane zgromadzone w Systemie powinny być sprostowane, uzupełnione lub usunięte zgodnie z procedurami, o których mowa w art. 35 rozporządzenia. Obowiązek ten będzie dotyczył organów uprawnionych, zgodnie z art. 3 rozporządzenia, do wprowadzania oraz modyfikowania danych, tj. Straży Granicznej, wojewody, Szefa Urzędu do Spraw Cudzoziemców, konsula oraz ministra właściwego do spraw zagranicznych.

Przyznanie Krajowej Jednostce ETIAS dostępu do danych EES ma na celu umożliwienie jej wykonywania zadań określonych w art. 25b rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniającego rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226, tj. wglądu do danych EES w celu analizowania i podejmowania decyzji w sprawie wniosków o zezwolenie na podróż. Z powodu umiejscowienia Krajowej Jednostki ETIAS w Straży Granicznej, uprawnienie to zostanie przyznane Straży Granicznej.

W projektowanym art. 4 określono podmioty uprawnione do pośredniego dostępu do KSI EES, tj. dostępu do danych przez wyznaczone organy państw członkowskich, które zgodnie z art. 29 ust. 1 rozporządzenia 2017/2226 są upoważnione do przeglądania danych EES w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie postępowań przygotowawczych. Dostęp taki jest możliwy w celu określonym w art. 32 ust. 2 rozporządzenia 2017/2226, tj. w celu identyfikacji nieznanej osoby podejrzanej o popełnienie przestępstwa terrorystycznego lub innego poważnego przestępstwa, nieznanego sprawcy takiego przestępstwa lub jego nieznanej domniemanej ofiary, lub w celu określonym w art. 32 ust. 3 rozporządzenia 2017/2226, tj. w celu przeglądania historii podróży lub okresów pobytu na terytorium państw członkowskich znanej osoby podejrzewanej o popełnienie przestępstwa terrorystycznego lub innego poważnego przestępstwa, znanego sprawcy takiego przestępstwa lub jego znanej domniemanej ofiary.

Ponieważ dostęp, o którym mowa w art. 4 projektu, jest przewidziany dla wyznaczonych organów, tj. zgodnie z definicją zawartą w art. 3 ust. 1 pkt 26 rozporządzenia 2017/2226 – organów wyznaczonych przez państwo członkowskie jako odpowiedzialne za zapobieganie przestępstwom terrorystycznym lub innym poważnym przestępstwom, za ich wykrywanie lub prowadzenie w ich sprawie postępowań przygotowawczych – uprawnienie to przysługuje prokuraturze, sądom, Policji, Straży Granicznej, Krajowej Administracji Skarbowej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Ochrony Państwa, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego i Żandarmerii Wojskowej.

Zgodnie z art. 32 ust. 2 rozporządzenia 2017/2226 wniosek o przeglądanie VIS w odniesieniu do tej samej osoby, której dane dotyczą, można złożyć jednocześnie z wnioskiem o dane EES, zgodnie z warunkami określonymi w decyzji Rady (WE) nr 2008/633/WSiSW.

Zaproponowane brzmienie przepisów art. 4 ust. 4 oraz art. 23 pkt 3 projektu ustawy jest wdrożeniem przedmiotowego postanowienia rozporządzenia 2017/2226.

Warto zaznaczyć, iż możliwość złożenia jednoczesnego wniosku o dane VIS istnieje tylko w przypadku wnioskowania do EES w celu identyfikacji nieznanej osoby podejrzanej o popełnienie przestępstwa terrorystycznego lub innego poważnego przestępstwa, nieznanego sprawcy takiego przestępstwa lub jego nieznanej domniemanej ofiary.

Zgodnie z art. 32 ust. 4 rozporządzenia 2017/2226 wyszukania w EES do celów identyfikacji można dokonać tylko według danych daktyloskopijnych i wizerunków twarzy.

Podkreślenia wymaga, iż nie ma możliwości zawnioskowania do CPD EES tylko o dane VIS.

Ponadto procedura realizacji dostępu do EES w trybie pośrednim zostanie opisana w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie sposobu i trybu dodawania jednostek operacyjnych oraz sposobu i trybu przyjmowania i rozpatrywania wniosków do Krajowej Jednostki ds. EES o dane EES przesyłanych w trybie pośrednim.

Jednocześnie warto zaznaczyć, że możliwość jednoczesnego wyszukania w EES i VIS do celów identyfikacji nie odbiera racji bytu Centralnych Punktów Dostępu do VIS dla Policji ani żadnego innego organu, wskazanych w art. 7 ust. 2 ustawy o udziale RP w SIS i VIS.

Standardowe wnioski o dane VIS nadal będą realizowane według zapisów ustawy o udziale RP w SIS i VIS oraz wydanych na jej podstawie aktów wykonawczych.

W odniesieniu do ust. 1 należy zauważyć, że art. 2 ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze określa, iż „Prokuratura wykonuje zadania w zakresie ścigania przestępstw oraz stoi na straży praworządności…”, a zatem będąc wyznaczonym organem zgodnie z art. 4 ust. 1, dane EES są przekazywane na wniosek wyznaczonych jednostek operacyjnych przez te organy. Przyjęte rozwiązanie, nieuwzględniające indywidualnie każdego z prokuratorów jako uprawnionego do dostępu do danych EES za pośrednictwem wyznaczonej przez siebie jednostki operacyjnej – wydaje się być zasadne z uwagi na wymagania, jakie musieliby spełnić, powołując każdy z osobna jednostkę operacyjną, która obsługiwałaby danego prokuratora.

W art. 5 wskazano, że Komendant Główny Straży Granicznej pełni funkcję Krajowej Jednostki ds. EES oraz wyznaczy komórkę organizacyjną Komendy Głównej Straży Granicznej realizującą zadania Krajowej Jednostki ds. EES, a także opisano jej zadania.

W art. 6 uregulowano wyznaczenie Centralnego Organu Technicznego KSI EES, który będzie realizował techniczne zadania wynikające z udziału Rzeczypospolitej Polskiej w Systemie oraz określono jego zadania, wynikające m.in. z art. 38 rozporządzenia 2017/2226. Jest to niezbędne dla prawidłowej organizacji, zarządzania i utrzymania infrastruktury krajowej EES, zapewnienia niezbędnych środków technicznych organom uprawnionym do przetwarzania danych oraz zapewnienie bezpiecznych rozwiązań technicznych. Na Centralny Organ Techniczny KSI EES zostały również nałożone obowiązki, w tym wynikające z art. 29 ust. 6 rozporządzenia 2017/2226 (prowadzenie ewidencji), art. 44 ust. 1, 3–5 rozporządzenia 2017/2226 (postępowanie w przypadku zaistnienia incydentów bezpieczeństwa).

Jednym z zadań COT KSI EES jest zapewnienie dostępu do danych EES przez aplikację WWW EES. Dostęp do danych EES via CPD nie jest ograniczony technicznie w kontekście liczby użytkowników końcowych, którzy mogą dokonywać zapytań w ramach organu uprawnionego. Opracowanie i utrzymanie aplikacji jest niezbędne w celu zapewnienia takiego dostępu.

Aplikacja WWW EES została zbudowana w sposób umożliwiający dostęp do systemu każdemu użytkownikowi końcowemu właściwie umocowanemu, tj. posiadającemu odpowiednie uprawnienia.

Dzięki takiemu rozwiązaniu nie ogranicza się liczby użytkowników końcowych w ramach poszczególnych instytucji. Decyzja dotycząca ilości użytkowników końcowych uprawnionych do danych EES pozostaje zawsze w gestii instytucji.

W projektowanym art. 7 ustawy określono zasady i sposób realizacji zadań wymienionych w art. 6.

Wyznaczenie jednego Centralnego Punktu Dostępu, zwanego dalej „CPD”, w Straży Granicznej, która została wskazana jako odpowiedzialna za wdrożenie systemu EES w Rzeczypospolitej Polskiej, jest zasadne ze względów prawnych, organizacyjnych i technicznych. Powyższe znalazło odzwierciedlenie zarówno w projekcie ustawy, jak i w zbudowanym „systemie krajowym”. Wyznaczenie jednego CPD do danych EES, usytuowanego w strukturze Straży Granicznej, zostało zaakceptowane przez Pełnomocnika Rządu ds. Systemów Wielkoskalowych, co z kolei stanowiło podstawę do rozpoczęcia przez Straż Graniczną działań zmierzających do budowy i wdrożenia Systemu.

Powołanie jednego CPD dla wszystkich wyznaczonych organów w Rzeczypospolitej Polskiej uzasadnione jest pod względem prawnym tym, że:

1. Straż Graniczna spełnia określone w rozporządzeniu 2017/2226 przesłanki, m.in. w zakresie sprawowania władzy publicznej;
2. Straż Graniczna będzie pełniła również funkcję wyznaczonego organu, co jest dopuszczalne w świetle art. 29 ust. 3 rozporządzenia 2017/2226;
3. wyznaczenie jednego CPD zapewnia większą niezależność od wyznaczonych organów niż w przypadku powołania kilku CPD;
4. proces legislacyjny w zakresie ustanowienia CPD jest ograniczony do jednego organu administracji rządowej, w ramach którego istnieje możliwość wyodrębnienia komórki organizacyjnej do wykonywania zadań CPD (jak pokazuje przykład Krajowej Jednostki do Spraw Informacji o Pasażerach w Komendzie Głównej Straży Granicznej);
5. wyodrębnienie CPD w niektórych organach administracji rządowej, szczególnie w służbach specjalnych, z uwagi na ich podległość pod różnych Ministrów, a także obowiązującą hierarchię służbową oraz wykonywanie ustawowych zadań mogłoby być utrudnione i skomplikowane.

Ponadto pod względem organizacyjnym powołanie jednego CPD:

1. powoduje zmiany struktury organizacyjnej jednego organu administracji rządowej;
2. ułatwia ustalenie jednolitych dla wszystkich wyznaczonych organów warunków dostępu do danych EES za pośrednictwem CPD;
3. skupia w jednym miejscu odpowiedzialność za realizację zadań nałożonych na CPD np. w zakresie prowadzenia wykazu jednostek operacyjnych uprawnionych do dostępu do danych EES za pośrednictwem CPD.

Umiejscowienie CPD w Komendzie Głównej Straży Granicznej jest rozwiązaniem korzystnym ze względu m.in. na:

1. jednolity nadzór nad przestrzeganiem przepisów w szczególności w zakresie:
2. dostępu wyznaczonych organów do danych EES,
3. rejestrowania i dokumentowania wszystkich operacji przetwarzania danych EES związanych z wnioskami wyznaczonych organów,
4. odpowiedniego upoważnienia osób mających dostęp do danych EES;
5. zapewnienie przez Straż Graniczną, jako administratora wyznaczonego na podstawie art. 39 ust. 1 rozporządzenia 2017/2226, właściwego nadzoru nad przetwarzaniem danych EES;
6. opracowanie jednego systemu wnioskowego dla wyznaczonych organów w zakresie:
7. wytworzenia, wdrożenia oraz utrzymania i rozwoju systemu (tworzenie oprogramowania i administracja oprogramowaniem, help desk, obsługa problemów, naprawa błędów itp.),
8. rozliczalności systemu,
9. przygotowywania sprawozdawczości dla Komisji Europejskiej (możliwość przygotowania dedykowanych raportów),
10. zarządzania użytkownikami i dostępu do danych EES (w przypadku formy scentralizowanej jest o wiele łatwiejsze i tańsze),
11. przygotowania rozwiązania opartego na eksploatowanej w SG architekturze i technologii będzie generowało niższe koszty,
12. obsługi informatycznej będzie rzutowało na niższe koszty utrzymania jednego CPD,
13. bezpieczeństwa przetwarzania i przechowywania danych EES;
14. możliwość skorzystania z posiadanego przez Straż Graniczną doświadczenia w zakresie budowy KSI PNR, w którym działa system wnioskowy (KSI PNR wraz z aplikacją dla organów właściwych („AOW”).

Istotną kwestią przemawiającą za stworzeniem jednego CPD są również koszty, jakie towarzyszą budowie, a następnie utrzymaniu systemu.

Pamiętać jednocześnie należy, że zasadniczym celem, jaki ma przyświecać realizacji projektu w całej Unii Europejskiej, jest przede wszystkim zapewnienie bezpieczeństwa obywatelom UE. Struktura zarządzania służbami w kontekście struktury administracyjnej kraju zdecydowanie wymaga zachowania jednolitego rozwiązania w budowaniu i utrzymywaniu systemów bezpieczeństwa, w tym krajowych komponentów systemów wielkoskalowych. Ujednolicenie dostępu do EES nie może być zatem odbierane jako utrudnienie dla służb publicznych, a jako wzmocnienie bezpieczeństwa w kontekście najlepszych praktyk dla budowania, utrzymania i eksploatowania systemów bezpieczeństwa zarówno w kontekście dostępu do samego EES, jak również w szerszym kontekście większego projektu, jakim jest wdrożenie ram interoperacyjności[[1]](#footnote-2)), zgodnie z zasadami bezpieczeństwa przetwarzania danach, rozliczalności, integralności i poufności.

Zastosowanie innej koncepcji wiązałoby się z koniecznością całkowitej przebudowy Systemu, dostosowania infrastruktury w służbach, a co za tym idzie brakiem możliwości zrealizowania testów EES i znacznym opóźnieniem we wdrożeniu EES oraz znacznymi kosztami dla Skarbu Państwa, a ponadto uniemożliwiłoby zastosowanie jednolitego działania i rozwiązywania problemów Systemu.

W art. 8 określono obowiązek informacyjny COT KSI EES, wynikający z art. 66 ust. 1 lit. c rozporządzenia. COT KSI EES, przed uruchomieniem KSI EES, poinformuje ministra właściwego do spraw wewnętrznych o gotowości KSI EES do produkcyjnego uruchomienia.

Art. 9 nakłada obowiązek współpracy określonych organów z COT KSI EES oraz KSI EES w celu realizacji zadań związanych z udziałem w EES, w tym odnośnie do przekazywania dokumentów, udzielania informacji oraz przekazywania aktualnych danych niezbędnych do prowadzenia wykazów jednostek organizacyjnych organów uprawnionych do przetwarzania danych EES i wszystkich jednostek operacyjnych mających dostęp do EES, a także zgłaszania ujawnionych nieprawidłowości w związku z przetwarzaniem danych EES przez KSI.

W art. 10 projektowanej ustawy określono obowiązek informacyjny, o którym mowa w art. 72 ust. 6 rozporządzenia. Zgodnie z przedmiotowym przepisem COT KSI EES będzie przedstawiał ministrowi właściwemu do spraw wewnętrznych, w terminie do dnia 31 marca każdego roku, informacje dotyczące technicznego funkcjonowania KSI EES w poprzednim roku kalendarzowym. Krajowa Jednostka ds. EES będzie przedstawiała ministrowi właściwemu do spraw wewnętrznych, w terminie do dnia 31 marca każdego roku, informacje dotyczące oceny funkcjonowania KSI EES w poprzednim roku kalendarzowym.

W art. 11, art. 12 i art. 14 wskazano organ sprawujący nadzór nad prawidłowością działania KSI EES oraz zakres uprawnień przyznanych w celu wykonywania nadzoru.

Art. 13 zawiera delegację ustawową do wydania przez ministra właściwego do spraw wewnętrznych rozporządzenia określającego sposób wykorzystywania KSI EES jako krajowego interfejsu EES.

W art. 15 zostały określone kwestie dotyczące wymogów wynikających z przepisów o ochronie danych osobowych. Zgodnie z projektowanym przepisem COT KSI EES, przed uruchomieniem KSI EES, występuje do Prezesa Urzędu Ochrony Danych Osobowych z wnioskiem o przeprowadzenie kontroli w zakresie spełniania przez KSI EES wymogów określonych w przepisach o ochronie danych osobowych. Określone zostały również prawa Prezesa Urzędu Ochrony Danych Osobowych, zastępcy Prezesa Urzędu lub upoważnionych przez niego pracowników w zakresie prowadzenia kontroli spełnienia przez KSI EES wymogów określonych w przepisach o ochronie danych osobowych. W przepisach projektowanego art. 15 określono także podmiot właściwy do wykonywania uprawnień, o których mowa w art. 84 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781). Prezes Urzędu Ochrony Danych Osobowych, wykonując powyższe uprawnienia, przedstawia COT KSI EES i Krajowej Jednostce ds. EES pisemną opinię w zakresie spełnienia przez KSI EES wymogów określonych w przepisach o ochronie danych osobowych, a w przypadku stwierdzenia nieprawidłowości w KSI EES przekazuje COT KSI EES i Krajowej Jednostce ds. EES zalecenia pokontrolne w formie pisemnej.

Art. 16 określa sposób postępowania w przypadku przedstawienia przez Prezesa Urzędu Ochrony Danych Osobowych zaleceń pokontrolnych. Zgodnie z projektowanym przepisem COT KSI EES i Krajowa Jednostka ds. EES mają prawo zgłoszenia na piśmie umotywowanych zastrzeżeń odnośnie do przekazanych zaleceń pokontrolnych, w terminie 7 dni od dnia otrzymania zaleceń pokontrolnych. W przypadku niezgłoszenia przez COT KSI EES lub Krajową Jednostkę ds. EES zastrzeżeń, jak również w przypadku nieuwzględnienia zastrzeżeń przez Prezesa Urzędu Ochrony Danych Osobowych, COT KSI EES lub Krajowa Jednostka ds. EES są obowiązane wykonać zalecenia pokontrolne, a następnie wystąpić z wnioskiem do organu, który przedstawił zalecenia pokontrolne, o przeprowadzenie kontroli, o której mowa w art. 15 ust. 1 projektowanej ustawy.

W art. 17 określono zasady bezpieczeństwa, w tym ochrony danych osobowych, które zdaniem projektodawcy skutecznie wyeliminują wszelkie niebezpieczeństwa, które mogłyby wpływać na realizację przepisów ustawy. W przepisie m.in.:

1. określono obowiązek wykonywania przez organ uprawniony do dostępu do KSI EES oraz przetwarzania danych poprzez KSI EES szkoleń wszystkich osób, które mają realizować to uprawnienie, w zakresie użytkowania KSI EES;
2. wskazano, że zadania administratora będzie wykonywała powołana w Komendzie Głównej Straży Granicznej komórka organizacyjna;
3. wprowadzono pojęcia użytkownika indywidualnego i końcowego, z uwagi na wykorzystywany przez użytkownika system umożliwiający dostęp do danych EES i związane z tym różne podmioty odpowiedzialne za zapewnienie rozliczalności działań użytkownika;
4. wskazano, jakie elementy powinny zawierać upoważnienia oraz doprecyzowano tryb nadawania upoważnień;
5. wskazano organ nadzorczy w zakresie ochrony danych osobowych na poziomie krajowym;
6. sprawy szkoleń pozostawiono do wewnętrznych ustaleń w każdym organie, który będzie miał prawo dostępu do EES, co pozwoli na lepsze zarządzanie czasem personelu w każdej organizacji. Dopuszczalne będzie wówczas np. połączenie kilku szkoleń z zakresu ochrony danych osobowych w jedno szkolenie, które będzie przeznaczone dla użytkowników różnych systemów wielkoskalowych. Powyższe pozwoli też na wprowadzanie dowolności w kontekście formy prowadzonych szkoleń, która może być różna w zależności od organu, np. szkolenia mogą odbywać się w formie stacjonarnej, zdalnej czy też hybrydowej. Warto także wskazać, że w rozporządzeniu 2017/2226 brak jest przepisów, które nakładałyby na państwa członkowskie obowiązek uregulowania, w tym przypadku w ustawie, kwestii szkoleń. W związku z powyższym zaproponowano wprowadzenie przepisów (ust. 1–3), które zdaniem projektodawcy w stopniu odpowiednim regulują ten obszar.

W ust. 10 określono kwestię nadawania i odbierania upoważnień, które pozostają w kompetencji właściwego organu, te zaś są uregulowane odrębnymi przepisami oraz zgodne z polityką bezpieczeństwa każdego z nich.

W ust. 16, w związku z przyjęciem rozwiązań w zakresie nadawania upoważnień dla użytkowników indywidualnych w formie elektronicznej, koniecznym było wypracowanie metod umożliwiających uprawnionym organom realizację tego procesu. W związku z powyższym definicja użytkownika indywidualnego, o której mowa w art. 2 pkt 21, wprowadza obok osoby upoważnianej do dostępu do danych EES również osobę upoważnioną do wnioskowania o nadanie lub cofnięcie upoważnienia dla użytkownika indywidualnego.

W odniesieniu do danych osobowych przetwarzanych poprzez KSI EES projekt przewiduje, że zastosowanie będą miały ogólne przepisy obowiązujące w tym zakresie z odrębnościami wynikającymi z rozporządzenia 2017/2226. Co do zasady zastosowanie będzie mieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwane dalej „RODO”) oraz ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781). Natomiast w przypadku przetwarzania danych osobowych w celu zwalczania przestępczości co do zasady zastosowanie będzie mieć ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).

W zakresie uprawnień obywateli państw trzecich, określonych w art. 15–18 RODO, tj. prawa dostępu do danych osobowych, ich sprostowania, uzupełnienia i usunięcia oraz do ograniczenia ich przetwarzania, projekt przewiduje, że wnioski o skorzystanie z tych uprawnień będą składane do administratora danych osobowych przetwarzanych przez KSI EES. Do rozpatrywania tych wniosków nie będzie mieć zastosowania ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572). Wnioski będą rozpatrywane na podstawie ogólnych przepisów regulujących kwestie przetwarzania danych osobowych, tj. RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, z wyjątkami wynikającymi z rozporządzenia 2017/2226.

Szczególne wymogi wynikające z art. 52 rozporządzenia 2017/2226 to 45-dniowy termin na rozpatrzenie wniosku, wymóg informowania wnioskodawców na piśmie o podjęciu czynności mających na celu rozpatrzenie złożonego wniosku, a w przypadku odmowy uwzględniania wniosku wymogi w zakresie uzasadnienia rozstrzygnięcia organu oraz pouczenia o przysługujących środkach zaskarżenia. Rozporządzenie 2017/2226 przewiduje również obowiązek prowadzenia określonego rejestru, który ma być udostępniany Prezesowi UODO.

Przepisy art. 52 ust. 4 i 5 rozporządzenia 2017/2226 posługują się wprawdzie pojęciem decyzji administracyjnej na określenie rozstrzygnięcia organu rozpatrującego wniosek obywatela państwa trzeciego, jednak w ocenie projektodawcy nie można uznać, że prawodawca unijny, przyjmując rozporządzenie 2017/2226, miał na myśli odwołania do konkretnych przepisów proceduralnych poszczególnych państw członkowskich, tj. w przypadku Polski do przepisów Kodeksu postępowania administracyjnego. W ocenie projektodawcy prawodawca unijny przez posłużenie się sformułowaniem decyzji administracyjnej miał na celu zapewnienie odpowiednich gwarancji podczas rozpatrywania wniosków obywateli państw trzecich dotyczących ich uprawnień w zakresie ich danych osobowych przetwarzanych przez EES, tj. rozpatrzenie wniosku w określonym terminie przez właściwy organ oraz zawarcie określonych informacji, które otrzymywać mają wnioskodawcy. W ocenie projektodawcy projektowana ustawa gwarantuje uwzględnienie wszystkich tych wymogów. Przysługujące obywatelom państw trzecich środki zaskarżenia określone są w RODO oraz ustawie o ochronie danych osobowych (skarga do Prezesa Urzędu do Spraw Ochrony Danych Osobowych lub sądu powszechnego).

Mając na uwadze przepisy prawa UE, które odwołują się do terminu *„system krajowy”* oraz podkreślanie przez Komisję Europejską „rozdzielności” technicznej, funkcjonalnej i logicznej zakresu obu systemów – krajowej odprawy (Krajowa Infrastruktura Graniczna) i EES, projektodawca, dążąc do najlepszych rozwiązań zmierzających do wdrożenia EES, przeanalizował możliwości techniczne i prawne służące zarówno zoptymalizowaniu samej odprawy granicznej, jak i związanych z nią procesów przetwarzania danych w Zintegrowanym Systemie Ewidencji 6 (system zawierający moduły odpraw granicznych oraz moduły obsługi administracyjnej cudzoziemców), zwanym dalej „ZSE6” – w tym archiwizowania w interesie publicznym danych osobowych.

Rozłączne rozwiązania krajowe w zakresie danych funkcjonujących w systemie odpraw oraz w EES pozwolą na zachowanie pełnej autonomii funkcjonowania krajowego systemu odpraw w celu realizacji zadań służbowych Straży Granicznej w oparciu o przepisy prawa krajowego i prawa UE, a także bez uszczerbku dla zasad ogólnych przechowywania danych pobranych z EES, jak również – przy zastosowaniu odpowiednich regulacji prawnych – pozwolą na przechowywanie danych pobranych z EES do ZSE6 na zasadzie wyjątku (motyw 36 i 37 rozporządzenia EES, o których mowa wyżej), a ponadto na przechowywanie danych, co do których zachodzi konieczność dłuższego ich przechowywania (dane w ZSE6) m.in. z uwagi na interes publiczny, do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Takie rozwiązanie będzie również wykonaniem zaleceń misji ewaluacyjnej Schengen przeprowadzonej w 2021 r. przez Komisję Europejską, wynikiem której były stwierdzone naruszenia związane z rejestracją w systemie odpraw obywateli Unii Europejskiej i członków ich rodzin, co – zdaniem misji ewaluacyjnej – stanowi ograniczenie swobody przemieszczania się, tj. naruszenie art. 21 Traktatu o funkcjonowaniu Unii Europejskiej (Dz. U. z 2004 r. poz. 864/2) i art. 5 ust. 1 dyrektywy 2004/38/WE Parlamentu Europejskiego i Rady w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium Państw Członkowskich, zmieniającej rozporządzenie (EWG) nr 1612/68 i uchylającej dyrektywy 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG i 93/96/EWG.

Mając na uwadze powyższe, a także złożoność materii dotyczącej wdrożenia EES oraz w dalszej perspektywie czasowej projekt o jeszcze większym stopniu skomplikowania, jakim jest wdrożenie ram interoperacyjności systemów wielkoskalowych, projektodawca uznał za konieczne jednolite uwzględnienie w przepisach prawa krajowego na poziomie ustawowym regulacji dotyczących Centralnego Systemu Informatycznego Straży Granicznej, jako nieodzownego instrumentu do pełnienia służby i wykonywania ustawowych zadań służbowych tej formacji.

**Zmiany w obowiązujących przepisach:**

Projekt zakłada wprowadzenie zmian w ustawie z dnia 6 kwietnia 1990 r. **o Policji** (Dz. U. z 2024 r. poz. 145, 1006, 1089, 1222, 1248 i 1473) w zakresie uprawnień Policji do przetwarzania danych biometrycznych w celach identyfikacji i weryfikacji tożsamości osób w związku z realizacją zadań ustawowych, co wynika z motywów 20, 21, 22 i 25 rozporządzenia 2017/2226.

W art. 20 ust. 1a ustawy z dnia 6 kwietnia 1990 r. o Policji zawarte jest ogólnie uprawnienie do przetwarzania tzw. danych wrażliwych. Proponuje się dodanie w art. 20 ust. 1aa, który wskazuje, że w celu realizacji zadań Policja będzie uprawniona do przetwarzania danych biometrycznych w postaci wizerunku twarzy oraz danych daktyloskopijnych. Uprawnienie do korzystania z tych danych będzie przysługiwało wyłącznie w celach identyfikacyjnych oraz w celu weryfikacji tożsamości osoby w zakresie określonym w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku zapobieganiem i zwalczaniem przestępczości.

Konieczność wprowadzenia wskazanej regulacji wynika z faktu, że często identyfikacja lub ustalenie tożsamości osoby za pomocą danych alfanumerycznych nie jest możliwe. Jak wynika z przepisów prawa Unii Europejskiej, systemy informacyjne, tj. SIS, VIS, czy też EES zawierają dane biometryczne w postaci wizerunków twarzy i danych daktyloskopijnych w celu korzystania z tych danych w celach identyfikacyjnych (tj. jednoznacznej identyfikacji lub weryfikacji tożsamości), wykrywczych lub dowodowych. Wizerunek twarzy osoby mający charakter danej biometrycznej jest przetwarzany w Rejestrze Dowodów Osobistych oraz w Rejestrze Dokumentów Paszportowych i dane te również służą do identyfikacji i ustalenia tożsamości osoby, która takim dokumentem się posługuje. Natomiast w ustawie o Policji obecnie brak jest przepisu określającego wprost uprawnienia Policji do korzystania z takich danych biometrycznych w postaci wizerunków twarzy i danych daktyloskopijnych we wskazanych powyżej celach w ramach zadań Policji, które wymagają jednoznacznej identyfikacji osoby lub weryfikacji jej tożsamości, a przepis art. 20 ust. 1a ustawy o Policji nie jest w tym zakresie wystarczający.

Przepis art. 20 ust. 1ab ma z kolei umożliwić Policji korzystanie z danych biometrycznych do realizacji jej zadań zgodnie z warunkami dostępu do tych danych wynikającymi z przepisów rozporządzeń UE. Dostęp do systemów informatycznych i do danych w nich zawartych, w tym w zakresie danych biometrycznych, jest realizowany, gdy wyczerpane zostały możliwości identyfikacyjne, wykrywcze lub dowodowe na poziomie krajowym, w tym z wykorzystaniem danych z krajowych baz danych, dlatego też niezbędne jest uregulowanie uprawnień Policji do przetwarzania wskazanych danych biometrycznych na poziomie krajowym w ustawie o Policji.

Proponowane zmiany w art. 20 ust. 1aa i 1ab oraz w art. 21nb są niezbędne dla zapewnienia Policji możliwości korzystania z danych zawartych w EES w pełnym zakresie, jaki daje ten system zgodnie z warunkami dostępu do tego systemu i pozostałych systemów UE, w tym z wykorzystaniem narzędzi interoperacyjności.

Zmiana w art. 21nb ustawy o Policji wiąże się ze zmianami w art. 20 ust. 1aa i 1ab tej ustawy i ma na celu uregulowanie wprost podstaw do przetwarzania danych biometrycznych w postaci wizerunków twarzy i danych daktyloskopijnych w zakresie umożliwiającym powiązania danych alfanumerycznych z danymi przetwarzanymi w zbiorach danych daktyloskopijnych, o których mowa w art. 21h ustawy o Policji. Przepis art. 21nb ustawy o Policji sankcjonuje uprawnienie Policji do przetwarzania wymienionych danych w KSIP właśnie w celach identyfikacyjnych, wykrywczych i dowodowych jako krajowego zbioru danych, z którego Policja korzysta w codziennej służbie i za pomocą którego dokonuje czynności związanych z ustaleniem tożsamości osoby, z uwagi na to, że system KSIP umożliwia uzyskiwanie danych z innych systemów, w tym z SIS. Jednocześnie należy wskazać, że identyfikacja osoby za pomocą danych daktyloskopijnych, która zwłaszcza w przypadku cudzoziemców jest często niezbędna do ich jednoznacznej identyfikacji, nie jest możliwa bez przetwarzania w KSIP informacji o danych daktyloskopijnych w postaci numeru AFIS i danych alfanumerycznych, w celu powiązania danych osoby z danymi daktyloskopijnymi przetwarzanymi w zbiorach danych daktyloskopijnych. Przepis art. 21nb ustawy o Policji ma na celu uregulowanie na poziomie krajowym uprawnień do korzystania z danych biometrycznych we wskazanych celach jako z krajowych baz danych, jak i z systemów informacyjnych UE, w tym EES, który dla Policji będzie niezbędnym systemem dla realizacji jej zadań związanych z zapobieganiem i zwalczaniem przestępczości.

W projekcie przyjęto rozwiązanie, w którym zamiast wskazywać konkretne przepisy prawa Unii Europejskiej, określające uprawnienia Policji do korzystania z danych z ECRIS-TCN, zastosowano na zasadzie analogii odwołanie odnoszące się do przetwarzania danych bez odniesienia się do konkretnych przepisów. Uszczegółowienie i dookreślenie spowodowałoby rozbieżność między dotychczasowym brzmieniem odwołującym się do systemów, z których korzysta Policja, a dookreśleniem dostępu do systemu ECRIS-TCN.

Ponadto wymagałoby to jednocześnie wskazania podstaw prawnych korzystania przez Policję z danych z pozostałych systemów wymienionych w tym przepisie, co spowodowałoby znaczną obszerność i nieczytelność projektowanej regulacji.

Wskazać również należy, że w celu dostosowania prawa krajowego do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiającego scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniającego rozporządzenie (UE) 2018/1726 powinna powstać regulacja uwzględniająca przepisy, zgodnie z którymi Policja na polecenie organów ścigania, w zakresie wykonywanych przez te organy zadań określonych w przepisach szczególnych, będzie pobierać odciski linii papilarnych od obywatela państwa trzeciego w rozumieniu art. 3 pkt 7 ww. rozporządzenia. Dane te będą przechowywane w zbiorach danych daktyloskopijnych w celu prowadzenia czynności identyfikacyjnych. Centralne Laboratorium Kryminalistyczne Policji w ramach swoich uprawnień będzie zatem przetwarzać dane osobowe, które będą przekazane za pośrednictwem Biura Informacyjnego Krajowego Rejestru Karnego z systemu ECRIS-TCN. Centralne Laboratorium Kryminalistyczne Policji nie będzie bezpośrednio korzystać z danych z systemu ECRIS, a jedynie przetwarzać dane przekazane przez Biuro Informacyjne Krajowego Rejestru Karnego bądź je do niego przekazywać.

Ustawa mająca na celu stosowanie przepisów rozporządzenia 2017/2226 pozostaje w związku z wdrożeniem jednoczesnego dostępu do VIS i EES i już na tym etapie jest związana z narzędziami interoperacyjności i związanym z tym przetwarzaniem danych z tych systemów. Dlatego też zasadne jest wprowadzenie proponowanych rozwiązań dotyczących uprawnień Policji do przetwarzania danych ze wskazanych systemów, które będzie się odbywało według zasad dostępu do tych systemów określonych w przepisach innych rozporządzeń Unii Europejskiej.

W ustawie z dnia 12 października 1990 r. **o Straży Granicznej** (Dz. U. z 2024 r. poz. 915, 1089, 1222, 1248 i 1473) niezbędne jest w szczególności zaktualizowanie brzmienia art. 1 ust. 2 pkt 9 w kontekście zmian dotyczących przetwarzania danych biometrycznych. Projekt dostosowuje również katalog zadań Straży Granicznej w związku z wykonywaniem zadań Krajowej Jednostki ds. EES i COT KSI EES oraz przetwarzania danych biometrycznych.

Projektowane przepisy są zasadne zarówno z punktu widzenia EES, prawa krajowego, a także przyszłych projektów dotyczących wielkoskalowych systemów informacyjnych UE.

Komisja Europejska stoi na stanowisku, że wszystkie Państwa Członkowskie powinny w tym zakresie posiadać jasne i klarowne prawo krajowe, które reguluje zarówno zakres (biometria), jak i czas przechowywania (i jest to tylko i wyłącznie właściwość krajowa). Przepisy w zakresie ochrony danych osobowych zasadniczo zabraniają przetwarzania danych wrażliwych, do których zalicza się również biometrię. Wyszczególniono jednak wyjątki, a spośród nich dla formacji Straży Granicznej istotny jest m.in. art. 9 ust. 2 lit. g rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO), w którym wskazano, iż można przetwarzać dane wrażliwe, jeżeli przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, ale na podstawie prawa Unii lub prawa państwa członkowskiego. Idąc dalej, w motywie 52 RODO wskazuje się, że należy również zezwolić na wyjątki od zakazu przetwarzania szczególnych kategorii danych osobowych – o ile przewiduje to prawo Unii lub prawo państwa członkowskiego (...). Także w art. 10 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 wskazuje się na możliwość przetwarzania danych biometrycznych pod warunkiem, że jest to dopuszczone prawem Unii lub prawem państwa członkowskiego, dlatego konieczne jest jednoznaczne ustawowe wskazanie, że Straż Graniczna może przetwarzać dane biometryczne.

Ponadto w projektowanej ustawie zdefiniowano CSI SG (Centralny System Teleinformatyczny SG), w oparciu o który funkcjonariusze SG wykonują zadania służbowe, oraz doprecyzowano terminy przechowywania danych osobowych. CSI SG obecnie funkcjonuje, jest utrzymywany i podlega ciągłej rozbudowie (jest to proces, co oznacza, że system będzie ewoluował wraz z potrzebami krajowymi i unijnymi, tak jak np. Krajowy Rejestr Cudzoziemców, który powstał jako system krajowy, a jest utrzymywany, rozbudowywany i modyfikowany również na potrzeby wielkoskalowych systemów UE). Administratorem CSI SG jest Komendant Główny Straży Granicznej. Obecnie zasadne jest stworzenie jednoznacznych, precyzyjnych regulacji ustawowych we wskazanym zakresie.

Projekt przewiduje również zmianę brzmienia art. 10a ustawy o Straży Granicznej przez dodanie do tego artykułu ust. 4a i 15a, w których określono zasady udostępniania danych biometrycznych. Wskazano podmioty, którym udostępnia się dane biometryczne, oraz dodatkowe warunki, jakie muszą spełniać m.in przez odwołanie się do ust. 9 w art. 10a, mając na względzie zapewnienie rozliczalności, zabezpieczeń technicznych i organizacyjnych. Jest to uzasadnione specyfiką wykonywanych zadań przez podmiot.

Dane biometryczne, które są przetwarzane i gromadzone w związku z m.in. kontrolą graniczną, wymagają zawężenia procesu ich przetwarzania do niezbędnego zakresu wykonywania ustawowych zadań. Przepisy wymagają, aby dane osobowe były adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane.

Zgodnie z art. 10 dyrektywy 2016/680 przetwarzanie danych wrażliwych, do których należą dane biometryczne, jest dozwolone jedynie po spełnieniu konkretnych warunków i wyłącznie wtedy, jeżeli jest to bezwzględnie niezbędne.

Dlatego projektowany art. 10a ust. 15a ustawy o Straży Granicznej zawęża udostępnianie danych biometrycznych do udostępniania tych danych wyłącznie w drodze teletransmisji, po wyrażeniu pisemnej zgody przez Komendanta Głównego Straży Granicznej na ich udostępnianie. Warunkiem takiego udostępnienia jest uprawnienie ustawowe podmiotu występującego do Komendanta Głównego Straży Granicznej o ich udostępnienie po spełnieniu, uregulowanych prawem, warunków technicznych.

Do prokuratury, której zadaniem jest przede wszystkim nadzór nad ściganiem przestępstw i postępowaniem karnym prowadzonym przez służby mundurowe, koordynacja działań związanych ze ściganiem przestępstw, sporządzanie aktów oskarżenia oraz prowadzenie spraw i występowanie w roli oskarżyciela przed sądem, nie stosuje się wymogu udostępniania danych biometrycznych wyłącznie w drodze teletransmisji, umożliwiając prokuraturze wnioskowanie o dane biometryczne w formie tradycyjnej, tj. każdorazowo na podstawie pisemnego wniosku.

Zatem, jeśli prokuratura wystąpi z pisemnym wnioskiem do Komendanta Głównego Straży Granicznej o udostępnienie jej tych danych, dane biometryczne zostaną prokuraturze udostępnione na podstawie pisemnego wniosku, a pisemna zgoda Komendanta nie będzie wymagana.

Projektowana ustawa zakłada zmiany w ustawie z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej, ustawie z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin oraz ustawie z dnia 12 grudnia 2013 r. o cudzoziemcach. Polegają one na wprowadzeniu do tych ustaw przepisów przewidujących obowiązki organów imigracyjnych i wizowych polegające na usuwaniu lub dodawaniu danych dotyczących obywateli krajów trzecich w Systemie, zgodnie z art. 19 oraz art. 35 ust. 6 rozporządzenia nr 2017/2226.

Nowelizacja ustawy z dnia 13 czerwca 2003 r. **o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej** (Dz. U. z 2023 r. poz. 1504 oraz z 2024 r. poz. 854) polega na dodaniu w art. 89n ust. 3 oraz w art. 110 ust. 8a, przewidujących usuwanie wpisów w EES, zgodnie z art. 35 ust. 6 rozporządzenia nr 2017/2226, w sytuacji uzyskania przez obywatela kraju trzeciego karty pobytu w związku z nadaniem mu statusu uchodźcy lub udzieleniem ochrony uzupełniającej w RP oraz w sytuacji wydania zaświadczenia potwierdzającego korzystanie z ochrony czasowej na podstawie tej ustawy, uprawniającego wraz z dokumentem podróży do wielokrotnego przekraczania granicy bez konieczności uzyskania wizy. Odnośnie do proponowanego art. 89n ust. 3 ww. ustawy należy wskazać, iż Szef Urzędu do Spraw Cudzoziemców wydający kartę pobytu obywatelowi kraju trzeciego, któremu nadano w Polsce status uchodźcy lub udzielono ochrony uzupełniającej, działa jako organ imigracyjny, a nie jako „organ rozstrzygający” zdefiniowany w art. 2 lit. f dyrektywy Parlamentu Europejskiego i Rady 2013/32/UE dnia 26 czerwca 2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej (Dz. Urz. UE L 180 z 29.06.2013, str. 60).

Zmiany w ustawie z dnia 14 lipca 2006 r. **o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin** (Dz. U. z 2024 r. poz. 633) przewidują usuwanie wpisów w EES, zgodnie z art. 35 ust. 6 rozporządzenia nr 2017/2226, w sytuacji, gdy będący obywatelem kraju trzeciego członek rodziny obywatela UE lub RP uzyska wizę krajową, kartę pobytową lub kartę stałego pobytu albo gdy obywatel Zjednoczonego Królestwa lub członek jego rodziny, będący beneficjentem Umowy Wystąpienia w Polsce, uzyska dokument pobytowy na podstawie tej ustawy. Usuwanie danych tych obywateli krajów trzecich z systemu EES przez właściwe organy w ww. sytuacjach przewiduje się w art. 8c oraz art. 10 ust. 6 tej ustawy. Ponadto w art. 10e w dodanym ust. 2 oraz w art. 73 ust. 5 ww. ustawy przewiduje się dodawanie danych w EES do ostatniego wpisu dotyczącego wjazdu/wyjazdu danego obywatela kraju trzeciego zarejestrowanego w EES, będącego członkiem rodziny obywatela UE lub RP albo obywatelem Zjednoczonego Królestwa lub członkiem jego rodziny, będącym beneficjentem Umowy Wystąpienia w Polsce, w przypadku cofnięcia lub unieważnienia okresu dozwolonego pobytu krótkoterminowego lub wizy Schengen, zgodnie z art. 19 ust. 1, 3 i 4 rozporządzenia nr 2017/2226, z uwzględnieniem definicji pojęcia cofnięcia lub unieważnienia pobytu krótkoterminowego, o którym mowa w art. 2 pkt 3 projektu.

Projektowana ustawa wprowadza zmiany dostosowujące w przepisach ustawy z dnia 24 sierpnia 2007 r. **o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym** (Dz. U. z 2023 r. poz. 1355), zwanej dalej „ustawą o SIS i VIS”.

Zmiana w art. 2 ustawy o SIS i VIS ma charakter wynikowy i ma na celu dodanie w tej ustawie definicji pojęć „dane EES” i „systemu EES”, używanych w projektowanych art. 7 ust. 3 i art. 7a ustawy o SIS i VIS. W art. 8 rozporządzenia 2017/2226 wskazano na interoperacyjność między systemami EES i VIS. Interoperacyjność między EES i VIS polega na utworzeniu bezpośredniego kanału komunikacyjnego między systemem centralnym VIS i systemem centralnym EES. W wyniku tych rozwiązań Straż Graniczna, która korzysta z EES, będzie mogła:

* przeglądać VIS w celu pobierania danych wizowych na potrzeby tworzenia lub aktualizowania wpisów dotyczących wjazdu/wyjazdu lub wpisów dotyczących odmowy wjazdu;
* weryfikować na granicach, na których działa EES, ważność wizy i tożsamość posiadacza wizy poprzez bezpośrednie porównanie jego odcisków palców z danymi przechowywanymi w VIS;
* weryfikować tożsamość obywateli państw trzecich zwolnionych z obowiązku wizowego poprzez porównanie ich odcisków palców z danymi przechowywanymi w VIS.

Identyczne uprawnienia zostały określone w art. 17a rozporządzenia 767/2008, który będzie stosowany z dniem wdrożenia EES.

Interoperacyjność powinna również umożliwić Straży Granicznej i organom wizowym, wskazanym w art. 5 ust. 1 ustawy o SIS i VIS (a więc Straży Granicznej, Szefowi Urzędu do Spraw Cudzoziemców, wojewodom, konsulom i Ministrowi Spraw Zagranicznych), które korzystają z VIS, bezpośrednie przeglądanie EES z poziomu VIS do celów rozpatrywania wniosków wizowych i podejmowania decyzji dotyczących tych wniosków oraz umożliwienia organom wizowym aktualizowania w EES danych wizowych w przypadku unieważnienia, cofnięcia lub przedłużenia wizy.

W związku z projektowanymi przepisami będzie istniała konieczność nowelizacji rozporządzenia ministra właściwego do spraw wewnętrznych, wydawanego na podstawie art. 25 ust. 12 ustawy o SIS i VIS, określającego tryb nadania dostępu do Krajowego Systemu Informatycznego (KSI) oraz tryb cofania tego dostępu, sposób przydzielania osobom uprawnionym osobistych i niepowtarzalnych identyfikatorów użytkownika indywidualnego, jak również sposób prowadzenia ewidencji użytkowników końcowych oraz użytkowników indywidualnych, a także wzór upoważnienia dla użytkownika indywidualnego do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych przez Krajowy System Informatyczny (KSI), przy uwzględnieniu konieczności zapewnienia bezpieczeństwa i ochrony przetwarzania danych przez Krajowy System Informatyczny (KSI), a więc rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 marca 2023 r. w sprawie dostępu i wzoru upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych przez Krajowy System Informatyczny (KSI) (Dz. U. poz. 424).

W ustawie z dnia 12 grudnia 2013 r. **o cudzoziemcach** (Dz. U. z 2024 r. poz. 769) proponuje się wprowadzenie w art. 79b, art. 139n ust. 13, art. 149b ust. 16, art. 156b ust. 14, art. 169a ust. 13 oraz w art. 248a przepisów przewidujących usuwanie przez właściwe organy wpisów danych obywateli krajów trzecich z systemu EES, gdy cudzoziemiec uzyska wizę krajową lub kartę pobytu albo korzysta z mobilności studenta lub z mobilności krótkoterminowej: pracownika przenoszonego wewnątrz przedsiębiorstwa, naukowca lub członka rodziny naukowca na terytorium Polski, zgodnie z art. 35 ust. 6 rozporządzenia nr 2017/2226. W art. 89a i art. 300 ust. 7 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach przewiduje się dodawanie danych w systemie EES do ostatniego wpisu dotyczącego wjazdu/wyjazdu danego obywatela kraju trzeciego zarejestrowanego w EES, w przypadku przedłużenia okresu dozwolonego pobytu krótkoterminowego lub wizy Schengen, przez organy właściwe w tych sprawach, zgodnie z art. 19 ust. 1, 2, 3 i 5 rozporządzenia nr 2017/2226. Natomiast w art. 96 ust. 3 oraz w art. 323 ust. 3 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach przewiduje się dodawanie danych w EES do ostatniego wpisu dotyczącego wjazdu/wyjazdu danego obywatela kraju trzeciego zarejestrowanego w EES, w przypadku cofnięcia lub unieważnienia okresu dozwolonego pobytu krótkoterminowego lub wizy Schengen, zgodnie z art. 19 ust. 1, 3 i 4 rozporządzenia nr 2017/2226, z uwzględnieniem definicji pojęcia cofnięcia lub unieważnienia pobytu krótkoterminowego, o którym mowa w art. 2 pkt 3 projektu. Z kolei zmiany w art. 300 ust. 2 i 6 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach mają na celu uwzględnienie brzmienia art. 20 ust. 2a i 2c Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. UE L 239 z 22.09.2000, str. 19, z późn. zm. – Dz. Urz. UE Polskie wydanie specjalne, rozdz. 19, t. 2, str. 9, z późn. zm.) wprowadzonych na mocy rozporządzenia nr 2017/2226. W art. 428 ust. 1 pkt 2 lit. p, art. 429, art. 430 i art. 449 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach przewiduje się regulacje dotyczące rejestru przedłużeń okresu pobytu w ramach ruchu bezwizowego, o których mowa w art. 300 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach, w celu ułatwienia realizacji projektowanego art. 300 ust. 7 tej ustawy. Rejestr ten będzie prowadzony w ramach krajowego zbioru rejestrów, ewidencji i wykazu w sprawach cudzoziemców, prowadzonego w systemie teleinformatycznym.

W odniesieniu do źródeł finansowania, o których mowa w pkt 6 OSR, należy wskazać, że Straż Graniczna prowadzi starania o pozyskanie środków z budżetu Unii Europejskiej na realizację wszystkich wyszczególnionych potrzeb. W ramach *Planu Dostosowania Organów Polskiej Administracji do Współpracy z przebudowanymi Wielkoskalowymi Systemami Informacyjnymi UE – MasterPlan* zaplanowany został do realizacji m.in. projekt pn. Wdrożenie systemu EES. Założenia finansowe do omawianego projektu wielkoskalowego opracowano w oparciu o realizowane na przestrzeni ostatnich lat w ww. obszarze umowy, przeprowadzone analizy rynku, które uwzględniały jednocześnie ryzyko inflacji i ryzyko walutowe (kurs USD oraz EUR). Jednakże należy mieć na uwadze, iż wskazane skutki finansowe są szacunkowe, w związku z tym dokonanie rozbicia tych skutków na poszczególne rodzaje wydatków może nie być wiążące i ulec zmianie w perspektywie wydłużonego okresu wejścia w życie regulacji.

Jednocześnie z uwagi na fakt, że wejście w życie projektowanej ustawy będzie powodowało skutki finansowe dla sektora finansów publicznych polegające na konieczności zwiększenia limitu wydatków, konieczne było zamieszczenie w treści normatywnej projektu stosownego przepisu dotyczącego reguły wydatkowej (tj. maksymalnego limitu tych wydatków wyrażonego kwotowo, na okres 10 lat budżetowych wykonywania ustawy, oddzielnie dla każdego roku). Maksymalny limit wydatków budżetu państwa w latach 2025–2034 będących skutkiem finansowym projektowanej ustawy określono na 380,833 mln zł, z czego w:

1) 2025 r. – 76,430 mln zł;

2) 2026 r. – 19,274 mln zł;

3) 2027 r. – 43,561 mln zł;

4) 2028 r. – 27,493 mln zł;

5) 2029 r. – 33,205 mln zł;

6) 2030 r. – 27,059 mln zł;

7) 2031 r. – 71,394 mln zł;

8) 2032 r. – 12,232 mln zł;

9) 2033 r. – 59,772 mln zł;

10) 2034 r. – 10,413 mln zł.

Maksymalny limit wydatków budżetu państwa w latach 2025–2034 będących skutkiem finansowym dla Komendanta Głównego Straży Granicznej określono na 265,127 mln zł. Zgodnie z projektem ustawy Komendant Główny Straży Granicznej będzie monitorował wykorzystanie ww. limitów wydatków, a w przypadku zagrożenia przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, wdroży mechanizm korygujący polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym ustawy, do poziomu zgodnego z limitem wydatków przyjętym dla danego roku budżetowego oraz kolejnych lat przez:

1) rozłożenie wymiany sprzętu na kolejne lata – w przypadku wymiany sprzętu;

2) zakup wsparcia do licencji na krótszy okres – w przypadku zakupu wsparcia do licencji.

Szczegółowy podział wydatków w latach 2025–2034:

1) 2025 r. – 43,734 mln zł;

2) 2026 r. – 13,943 mln zł;

3) 2027 r. – 40,000 mln zł;

4) 2028 r. – 23,000 mln zł;

5) 2029 r. – 24,950 mln zł;

6) 2030 r. – 19,500 mln zł;

7) 2031 r. – 33,500 mln zł;

8) 2032 r. – 7,500 mln zł;

9) 2033 r. – 55,000 mln zł;

10) 2034 r. – 4,000 mln zł.

Maksymalny limit wydatków budżetu państwa w latach 2025–2034 będących skutkiem finansowym dla Ministerstwa Spraw Wewnętrznych i Administracji określono na 7,146 mln zł. Zgodnie z projektem ustawy minister właściwy do spraw wewnętrznych będzie monitorował wykorzystanie ww. limitów wydatków, a w przypadku gdy wielkość wydatków po trzech kwartałach wyniesie łącznie więcej niż 75% limitu przewidzianego na dany rok, wielkość wydatków w IV kwartale obniży o kwotę przekroczenia, określając zakres ograniczeń dla poszczególnych zadań realizowanych na podstawie ustawy. Szczegółowy podział wydatków w latach 2025–2034:

1) 2025 r. – 0,536 mln zł;

2) 2026 r. – 0,601 mln zł;

3) 2027 r. – 0,631 mln zł;

4) 2028 r. – 0,663 mln zł;

5) 2029 r. – 0,695 mln zł;

6) 2030 r. – 0,729 mln zł;

7) 2031 r. – 0,764 mln zł;

8) 2032 r. – 0,802 mln zł;

9) 2033 r. – 0,842 mln zł;

10) 2034 r. – 0,883 mln zł;

Maksymalny limit wydatków budżetu państwa w latach 2025–2034 będących skutkiem finansowym dla Urzędu do Spraw Cudzoziemców określono na 108,56 mln zł. Zgodnie z projektem ustawy Urząd do Spraw Cudzoziemców będzie monitorował wykorzystanie ww. limitów wydatków, a w przypadku gdy wielkość wydatków po trzech kwartałach wyniesie łącznie więcej niż 75% limitu przewidzianego na dany rok, wielkość wydatków w IV kwartale obniży o kwotę przekroczenia, określając zakres ograniczeń dla poszczególnych zadań realizowanych na podstawie ustawy. Szczegółowy podział wydatków w latach 2025–2034:

1) 2025 r. – 32,160 mln zł;

2) 2026 r. – 4,730 mln zł;

3) 2027 r. – 2,930 mln zł;

4) 2028 r. – 3,830 mln zł;

5) 2029 r. – 7,560 mln zł;

6) 2030 r. – 6,830 mln zł;

7) 2031 r. – 37,130 mln zł;

8) 2032 r. – 3,930 mln zł;

9) 2033 r. – 3,930 mln zł;

10) 2034 r. – 5,530 mln zł;

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

* art. 3 ust. 1 pkt 8, który wejdzie w życie z dniem określonym w decyzji Komisji Europejskiej, zgodnie z art. 88 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniającego rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226 (Dz. Urz. UE L 236 z 19.09.2018, str. 1);
* art. 19 pkt 1 w zakresie dodawanego ust. 1ab w art. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji w części dotyczącej dostępu do systemu ECRIS-TCN, który wchodzi w życie z dniem określonym w decyzji Komisji Europejskiej, zgodnie z art. 35 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiającego scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniającego rozporządzenie (UE) 2018/1726 oraz
* art. 5 ust. 1 i ust. 2 pkt 2 i 5, art. 6 ust. 2 pkt 1 i 3, art. 8, art. 12 i art. 15–17, które wejdą w życie z dniem następującym po dniu ogłoszenia. W związku z potrzebą wejścia w życie tych przepisów jeszcze przed datą uruchomienia Systemu zdecydowano się skorzystać z przewidzianej w art. 4 ust. 2 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461) możliwości skrócenia *vacatio legis*. Zgodnie z ww. przepisem w uzasadnionych przypadkach akty normatywne mogą wchodzić w życie w terminie krótszym niż czternaście dni, a jeżeli ważny interes państwa wymaga natychmiastowego wejścia w życie aktu normatywnego i zasady demokratycznego państwa prawnego nie stoją temu na przeszkodzie, dniem wejścia w życie może być dzień ogłoszenia tego aktu w dzienniku urzędowym.

Projektowana ustawa nie będzie miała wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorców.

Projekt został udostępniony w Biuletynie Informacji Publicznej na stronie internetowej Rządowego Centrum Legislacji, w zakładce „Rządowy Proces Legislacyjny”, zgodnie z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806) oraz stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248). W trybie przepisów o działalności lobbingowej w procesie stanowienia prawa żaden z podmiotów nie zgłosił zainteresowania nad projektem.

Projektowany akt prawny nie podlega procedurze notyfikacji określonej w przepisach rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.).

Projektowany akt prawny nie wymaga przedłożenia właściwym instytucjom i organom UE, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

1. ) W związku z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze granic i polityki wizowej oraz zmieniającym rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726, (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz. Urz. UE L 135 z 22.05.2019, str. 27). [↑](#footnote-ref-2)