Zalecenia Schengen dla Polski w obszarze ochrony danych osobowych

Posted on 2025-02-28

Polska zasadniczo spełnia wymogi w zakresie ochrony danych w dorobku Schengen. Są jednak niedociągnięcia, na które nasz kraj musi zwrócić uwagę.

Eksperci Komisji Europejskiej i państw członkowskich przeprowadzili od marca do kwietnia 2024 r. ocenę stosowania przez Polskę dorobku Schengen. Procedura ta obejmowała także ochronę danych osobowych. Wynikiem tego działania jest sprawozdanie z oceny stosowania przez Polskę dorobku Schengen w 2024 r., które zostało przyjęte przez Komisję Europejską.

Czym jest mechanizm oceny dorobku Schengen?

Strefa bez kontroli na granicach wewnętrznych opiera się na skutecznym i wydajnym stosowaniu przepisów Schengen przez państwa członkowskie. Zasady te obejmują:

- • środki zabezpieczające granice zewnętrzne,
- • środki kompensujące brak kontroli na granicach wewnętrznych,
- • oraz solidne ramy monitorowania.
  Środki te wzmacniają swobodę przemieszczania się i zapewniają wysoki poziom bezpieczeństwa, sprawiedliwości i ochrony praw podstawowych, w tym ochrony danych osobowych.

  Mechanizm oceny i monitorowania Schengen jest kluczowym zabezpieczeniem zapewniającym dobre funkcjonowanie strefy Schengen. Zespół składający się z ekspertów z państw członkowskich i Komisji raz na siedem lat ocenia każde państwo członkowskie i państwo stowarzyszone w ramach Schengen pod kątem pełnego stosowania przepisów Schengen. Po przeprowadzeniu oceny Komisja sporządza sprawozdanie, które zawiera zalecenia dotyczące działań naprawczych, jakie powinien podjąć oceniany kraj, a także priorytety ich wdrożenia i terminy realizacji.

  W 2022 r. przyjęto nowe ramy ocen Schengen, co doprowadziło do bardziej usprawnionych i kompleksowych zaleceń dla poszczególnych krajów. Zapoczątkowało to trzecią generację ocen Schengen. Wstępny harmonogram weryfikacji stosowania przepisów Schengen w każdym kraju UE został określony w wieloletnim programie oceny na lata 2023-2029 i jego zmianach. W uzupełnieniu i potwierdzeniu tego planowania przyjmowane są roczne programy ewaluacji, zawierające szczegółowe harmonogramy ewaluacji przeprowadzanych w danym roku.

Jak wypada Polska?

Jak zauważyli ewaluatorzy, wojna w Ukrainie ma istotny wpływ na wdrażanie przez Polskę dorobku Schengen, ponieważ nasz kraj jest odpowiedzialny za zabezpieczenie odcinka granicy z Ukrainą, który jest dotknięty bezprecedensowym napływem osób ubiegających się

o ochronę międzynarodową i stosujący specjalny system ochrony ustanowiony przez UE. Pomimo złożonego otoczenia i wyzwań Polska skutecznie wdraża dorobek Schengen i zapewnia znaczący wkład w funkcjonowanie strefy Schengen. Komisja Europejska wraz z ekspertami państw członkowskich stwierdziła, że Polska zasadniczo spełnia wymogi w zakresie ochrony danych. Stwierdzone niedociągnięcia dotyczą głównie:

- wyłączenia z zakresu stosowania polskiej ustawy transponującej dyrektywę o ochronie danych w sprawach karnych niektórych rodzajów przetwarzania danych osobowych w niektórych dziedzinach prawa krajowego oraz niektórych organów w zakresie, w jakim dotyczy to również danych przetwarzanych w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym (VIS);
- braku odzwierciedlenia ról i obowiązków Centralnego Organu Technicznego Krajowego Systemu Informatycznego (COT KSI) i właściwych organów jako współadministratorów w odniesieniu do przetwarzania danych osobowych w SIS i VIS, co skutkuje pewnymi niedociągnięciami w zakresie nadzoru nad całymi systemami, takimi jak brak skutecznego monitorowania własnej działalności;
- braku pośredniego dostępu do danych w SIS za pośrednictwem Urzędu Ochrony Danych Osobowych, w przypadku gdy odmówiono dostępu do danych osobowych, ich sprostowania lub usunięcia oraz braku sądowego środka ochrony prawnej w odniesieniu do odpowiedzi administratora na wnioski osób, których dane dotyczą, w kontekście SIS i VIS.

Z oceny wynika, że obszarami priorytetowymi dla Polski z zakresu ochrony danych osobowych są: dostosowanie zakresu polskiej ustawy transponującej dyrektywę o ochronie danych w sprawach karnych w zakresie, w jakim ma ona wpływ na przetwarzanie danych osobowych w SIS i VIS, oraz zagwarantowanie skutecznego mechanizmu monitorowania własnej działalności przez COT-KSI i właściwe organy.

W wyniku okresowej oceny Polski z 2024 r. sformułowano 105 zaleceń dotyczących działań naprawczych mających na celu wyeliminowanie przez Polskę niedociągnięć i wyeliminowanie obszarów wymagających poprawy wskazanych w sprawozdaniu z oceny. W

zakresie ochrony danych osobowych zalecenia dla Polski dotyczą m.in:

- zapewnienia pełnej transpozycji dyrektywy (UE) 2016/680 w odniesieniu do przetwarzania danych osobowych wymienionych w art. 3 pkt. 1 polskiej ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości; ponadto należy zapewnić transpozycję dyrektywy (UE) 2016/680 również w odniesieniu do danych osobowych przetwarzanych na podstawie dorobku Schengen przez organy wymienione w art. 3 pkt. 2 polskiej ustawy z dnia 14 grudnia 2018 r., np. przetwarzanie danych osobowych z SIS i VIS do celów wymienionych w dorobku prawnym dotyczącym SIS i VIS; (zalecenie priorytetowe)
- zapewnienia, aby osoby, których dane dotyczą, mogły wykonywać swoje prawa dostępu do danych osobowych w Systemie Informacyjnym Schengen, ich sprostowania i usunięcia za pośrednictwem Urzędu Ochrony Danych Osobowych, w przypadku gdy administrator odmówił takiego dostępu do danych osobowych przetwarzanych w Systemie Informacyjnym Schengen, ich sprostowania lub usunięcia zgodnie z art. 53 ust. 3 rozporządzenia (UE) 2018/1861 i art. 67 ust. 3 rozporządzenia (UE) 2018/1862 oraz art. 19 rozporządzenia (UE) 2018/1860; (zalecenie priorytetowe)
- zagwarantowania, by osoby, których dane dotyczą, mogły korzystać z prawa do skutecznego środka ochrony prawnej przed sądem przeciwko decyzji administratora dotyczącej praw osób, których dane dotyczą, oraz by były informowane o tym prawie w odpowiedzi administratora zgodnie z art. 53 ust. 3 i art. 54 ust. 1 rozporządzenia (UE) 2018/1861, art. 67 ust. 3 i art. 68 ust. 1 rozporządzenia (UE) 2018/1862 oraz art. 19 rozporządzenia (UE) 2018/1860; (zalecenie priorytetowe)
- zapewnienia, aby role i obowiązki Centralnego Organu Technicznego Krajowego Systemu Informatycznego (Komendant Główny Policji) i właściwych organów w odniesieniu do przetwarzania danych osobowych SIS zostały wyjaśnione w prawie i praktyce zgodnie z art. 24 i 26 rozporządzenia (UE) 2016/679 oraz art. 19 i 21 dyrektywy (UE) 2016/680;
- dokonania oceny we współpracy z Urzędem Ochrony Danych Osobowych prawa Centralnego

Biura Antykorupcyjnego do wprowadzania do SIS wpisów związanych z zagrożeniami dla bezpieczeństwa narodowego;

- zapewnienia, aby wszystkie organy przetwarzające dane SIS i korzystające z niego proaktywnie, regularnie i wyrywkowo sprawdzały rejestry dotyczące wszystkich działań użytkowników w oparciu o skoordynowane podejście;
- proaktywnego informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych w SIS i VIS oraz o wykonywaniu ich praw (np. w postaci ulotek, plakatów) w komendach policji i na lotniskach;
- zapewnienia, aby Centralny Organ Techniczny Krajowego Systemu Informatycznego – Komendant Główny Policji (administrator COT KSI) znalazł alternatywną procedurę dla polskiej Elektronicznej Platformy Usług Administracji Publicznej (ePUAP) w odniesieniu do elektronicznego wniosku o realizację praw osób, których dane dotyczą, tak aby osoby, których dane dotyczą, bez możliwości złożenia wniosku za pośrednictwem ePUAP, mogły również wykonywać swoje prawa osób, których dane dotyczą, drogą elektroniczną;
- zapewniła, aby wszystkie zalecenia dotyczące aspektów ochrony danych związanych z zarządzaniem krajowego SIS były również przedmiotem działań naprawczych w związku z zarządzaniem krajowego VIS.

Działania następcze i monitorowanie

W ciągu dwóch miesięcy od przyjęcia sprawozdania państwo członkowskie jest zobowiązane do przedłożenia planu działania określającego, w jaki sposób zamierza naprawić zidentyfikowane niedociągnięcia. Po konsultacji z zespołem, który przeprowadził działanie w zakresie oceny, Komisja przedstawi Polsce analizę adekwatności planu działań w terminie miesiąca od jego przedłożenia. Jeżeli Komisja uzna, że plan działań nie jest adekwatny,

Polska będzie musiała przedłożyć zmieniony plan działań w terminie miesiąca od otrzymania wyników analizy. Komisja przedstawi również analizę planu działań Radzie UE. Od dnia potwierdzenia otrzymania analizy planu działań Polska będzie składać Komisji Europejskiej i Radzie sprawozdanie z realizacji swojego planu działań co sześć miesięcy aż do momentu, gdy Komisja uzna, że plan działań został w pełni zrealizowany. Plan działań naprawczych zostanie zamknięty, w przypadku gdy Komisja uzna, że plan działań został w pełni zrealizowany, o czym Polska zostanie poinformowana.

Plan kontroli sektorowych UODO

Warto przy tej okazji przypomnieć, że przetwarzanie danych osobowych w Wielkoskalowych Systemach Informacyjnych Unii Europejskiej, w tym przetwarzanie danych osobowych SIS/VIS podlega kontroli sektorowej UODO, zgodnie z przyjętym przez Prezesa UODO planem na 2025 r.

Źródła:

Schengen Evaluation and Monitoring Mechanism

Schengen Evaluation of POLAND

Podstawa prawna:

Rozporządzenie Rady (UE) 2022/922 z dnia 9 czerwca 2022 r. w sprawie ustanowienia i funkcjonowania mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz w sprawie uchylenia rozporządzenia (UE) nr 1053/2013