Rada
Unii Europejskiej

Bruksela, 25 czerwca 2026 r.
(OR. en)

11080/26

Międzyinstytucjonalny numer referencyjny:
2026/0173 (COD)

DATAPROTECT 219
JAI 879
COPEN 244
IXIM 146
ENFOPOL 241

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	23 czerwca 2026 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2026) 314 final
Dotyczy:	Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY zmieniające Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych.

Delegacje otrzymują w załączeniu dokument COM(2026) 314 final.

Zał.: COM(2026) 314 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 23.6.2026 r.
COM(2026) 314 final

2026/0173 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

zmieniające Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych.

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Rozporządzenie (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii (rozporządzenie (UE) 2018/1725) opracowano w celu ustanowienia spójnego i zmodernizowanego systemu ochrony danych dla wszystkich instytucji, organów i jednostek organizacyjnych Unii. Rozdział IX rozporządzenia (UE) 2018/1725 przewidziano konkretnie w celu uregulowania „operacyjnych danych osobowych" (tj. danych osobowych przetwarzanych na potrzeby wykonywania czynności, które wchodzą w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE) przez agencje i organy Unii w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (WSiSW), w tym Europol, Eurojust, Prokuraturę Europejską (EPPO) oraz, w ograniczonym zakresie, Frontex.

Ramy ochrony danych mające zastosowanie do agencji i organów UE w dziedzinie WSiSW – mimo przyjęcia rozporządzenia (UE) 2018/1725 – pozostają rozdrobnione. W szczególności rozdział IX nie ma zastosowania do EPPO, w przypadku której rozporządzenie ustanawiające weszło w życie przed rozporządzeniem (UE) 2018/1725. W rezultacie niektóre przepisy rozporządzenia w sprawie EPPO różnią się co do istoty od odpowiadających im przepisów określonych w rozdziale IX rozporządzenia (UE) 2018/1725 lub są sformułowane w inny sposób. Rozporządzenie (UE) 2018/1725 stanowi ponadto, że w odniesieniu do przetwarzania operacyjnych danych osobowych zastosowanie ma wyłącznie art. 3 (definicje) i rozdział IX. Z jednej strony doprowadziło to do tego, że w aktach ustanawiających odpowiednich organów lub jednostek organizacyjnych utrzymano przepisy regulujące niektóre aspekty związane z przetwarzaniem operacyjnych danych osobowych. Z drugiej strony doprowadziło to do niepewności prawa co do tego, czy i w jakim zakresie przepisy zawarte w rozdziałach II–VIII, takie jak przepisy dotyczące rejestrów czynności przetwarzania lub zadań inspektora ochrony danych, mają zastosowanie w sytuacjach, w których analogiczne przepisy nie istnieją ani w rozdziale IX, ani w aktach ustanawiających odpowiednich organów lub jednostek organizacyjnych. Taka fragmentacja przepisów nie tylko podważa pewność prawa, ale również stwarza praktyczne przeszkody dla skutecznej współpracy między organami i jednostkami organizacyjnymi Unii przy wymianie danych. W pierwszym sprawozdaniu ze stosowania rozporządzenia (UE) 2018/1725 z 2022 r. Komisja uznała te niedociągnięcia i rozważyła interwencję ustawodawczą w celu ich wyeliminowania.

W tym kontekście celem niniejszego wniosku jest uproszczenie i zapewnienie spójności obowiązujących ram ochrony danych, w szczególności poprzez dostosowanie odpowiednich przepisów we wszystkich organach i jednostkach organizacyjnych Unii. Oczekuje się, że dostosowanie to zmniejszy obciążenia administracyjne i ułatwi wymianę danych między organami i jednostkami organizacyjnymi Unii, a jednocześnie zwiększy pewność prawa. W interesie spójności i zgodnie z ogólnym celem, jakim jest zminimalizowanie fragmentacji przepisów o ochronie danych, wniosek opiera się na następujących czterech głównych celach:

Zapewnienie spójnego stosowania ochrony danych we wszystkich instytucjach, organach, urzędach i agencjach UE

Należy rozszerzyć zakres zastosowania rozdziału IX, aby zapewnić jego spójne stosowanie we wszystkich agencjach, organach i urzędach UE w sektorze wymiaru sprawiedliwości w sprawach karnych i egzekwowania prawa. Pozwoli to włączyć Prokuraturę Europejską do ram rozporządzenia (UE) 2018/1725. Odbędzie się to bez uszczerbku dla możliwości utrzymania w rozporządzeniu w sprawie EPPO szczegółowych przepisów o ochronie danych

niezbędnych do odzwierciedlenia wyjątkowego charakteru EPPO jako niezależnej prokuratury Unii. Przepisy zawarte w rozdziale IX są już dostosowane do odpowiednich przepisów dyrektywy (UE) 2016/680 o ochronie danych w sprawach karnych i doprowadzą do powstania jednolitego, zharmonizowanego zbioru przepisów dla wszystkich zainteresowanych stron w celu zmniejszenia fragmentacji i zapewnienia spójności stosowanych przepisów.

Większa pewność prawa

W rozdziale IX brakuje obecnie przepisów dotyczących kilku ważnych aspektów, w tym dotyczących roli inspektorów ochrony danych, prowadzenia rejestrów czynności przetwarzania, współpracy między organami nadzorczymi oraz międzynarodowego przekazywania operacyjnych danych osobowych. Celem wniosku jest konsolidacja przepisów w jednym miejscu, aby usprawnić ich przestrzegani bez wywierania znaczącego wpływu operacyjnego. Zapewni ona również większą jasność administratorom, podmiotom przetwarzającym i osobom, których dane dotyczą.

Uporządkowanie uprawnień Europejskiego Inspektora Ochrony Danych

Uprawnienia nadzorcze EIOD są obecnie uregulowane w aktach ustanawiających Europol, Eurojust i EPPO; każdy z tych aktów zawiera rozbieżne przepisy, co prowadzi do niepewności i nieefektywności. Akt ustanawiający Frontex nie reguluje nadzoru EIOD nad przetwarzaniem danych operacyjnych, co prowadzi do znacznej asymetrii.

Wniosek doprecyzowuje, że EIOD otrzymuje uprawnienia nadzorcze odpowiadające uprawnieniom określonym w art. 58 rozporządzenia (UE) 2018/1725, ale dostosowane do kontekstu przetwarzania danych operacyjnych, w szczególności względem Prokuratury Europejskiej w kontekście działań związanych z prowadzeniem postępowań przygotowawczych oraz wnoszeniem i popieraniem oskarżeń. W tym względzie wniosek opiera się na modelu uprawnień EIOD z reformy Europolu z 2022 r., przy jednoczesnym zapewnieniu spójności z rozdziałem VI rozporządzenia (UE) 2018/1725 i dyrektywą o ochronie danych w sprawach karnych. We wniosku usuwa się z aktów ustanawiających przepisy dotyczące zadań i uprawnień EIOD odnoszące się do poszczególnych agencji.

Ogólne uporządkowanie

Celem wniosku jest ponadto uporządkowanie przepisów w celu wyeliminowania zbędnych, powielających się i niespójnych przepisów w dziedzinie ochrony danych w odniesieniu do organów i jednostek organizacyjnych Unii w dziedzinie WSiSW podczas prowadzenia działań wchodzących w zakres części trzeciej tytuł V rozdziały 4 i 5 TFUE. W stosownych przypadkach dostosowuje on również przepisy dotyczące przetwarzania danych operacyjnych do wniosku dotyczącego aktu zbiorczego prawa cyfrowego[(1)].

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Wniosek ma na celu dostosowanie przepisów rozporządzenia (UE) 2018/1725 do istniejących polityk ochrony danych, wzmacniając zasady ustanowione w ogólnym rozporządzeniu o ochronie danych (RODO) i dyrektywie o ochronie danych w sprawach karnych. W stosownych przypadkach zapewnia on dostosowanie do zmian ram ochrony danych zaproponowanych w akcie zbiorczym prawa cyfrowego.

---

(1) Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie zmiany rozporządzeń (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 oraz dyrektyw 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do uproszczenia cyfrowych ram prawnych oraz uchylenia rozporządzeń (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 i dyrektywy (UE) 2019/1024 (akt zbiorczy prawa cyfrowego), 19.11.2025, COM(2025) 837 final.

- **Spójność z innymi politykami Unii**

Wniosek jest częścią pakietu inicjatyw w zakresie wymiaru sprawiedliwości w sprawach karnych służących realizacji spójnego i uzupełniającego się celu: wzmocnienia zdolności Unii do zapobiegania poważnej przestępczości transgranicznej, jej wykrywania, prowadzenia postępowań przygotowawczych w jej sprawie i wnoszenia w jej sprawie oskarżeń w coraz bardziej złożonym środowisku bezpieczeństwa. Poprzez modernizację ram prawnych regulujących współpracę między organami ścigania, organami sądowymi i innymi odpowiednimi organami pakiet ma służyć zwiększeniu skuteczności, spójności i interoperacyjności unijnej architektury bezpieczeństwa wewnętrznego.

Proponowane zmiany rozporządzeń w sprawie Europolu i Eurojustu stanowią podstawę tego projektu. Europol i Eurojust pełnią w przestrzeni wolności, bezpieczeństwa i sprawiedliwości odrębne, lecz uzupełniające się funkcje: Europol wspiera zapobieganie działalności przestępczej, jej wykrywanie i prowadzenie postępowań przygotowawczych w jej sprawie, natomiast Eurojust ułatwia współpracę wymiarów sprawiedliwości i zapewnia skuteczne działania następcze w zakresie ścigania przestępstw i wymiaru sprawiedliwości. Pakiet ma zatem służyć wzmocnieniu współpracy i komplementarności między obiema agencjami, oraz z innymi odpowiednimi podmiotami unijnymi w obszarach wymiaru sprawiedliwości i spraw wewnętrznych oraz struktury zwalczania nadużyć finansowych, co ma przekładać się na płynne przejście między działaniami organów ścigania a działaniami sądowymi na wszystkich etapach łańcucha wymiaru sprawiedliwości w sprawach karnych.

W tym kontekście zmiany ram europejskiego nakazu dochodzeniowego i niniejszy wniosek dodatkowo służą osiągnięciu tego celu poprzez ułatwienie skutecznej współpracy transgranicznej, poprawę warunków wymiany informacji i zapewnienie spójnych ram prawnych dostosowanych do realiów operacyjnych i rozwoju technologicznego. Wszystkie razem środki zaproponowane w niniejszym pakiecie zwiększą zdolność Unii do reagowania na zmieniające się zagrożenia dla bezpieczeństwa, przy pełnym poszanowaniu praw podstawowych, praworządności i podziału obowiązków między różnymi zaangażowanymi podmiotami.

W niniejszym wniosku określono w szczególności wszystkie wspólne elementy przepisów o ochronie danych mających zastosowanie do Europolu i Eurojustu oraz zgrupowano je w rozporządzeniu (UE) 2018/1725, eliminując tym samym fragmentację i powielanie. W aktach ustanawiających organów i jednostek organizacyjnych Unii działających w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych pozostaną wyłącznie przepisy o ochronie danych opracowane w celu odzwierciedlenia ich odpowiednich szczególnych potrzeb operacyjnych i charakteru.

Przyjęcie wniosku następuje równolegle ze zmianami rozporządzeń w sprawie Europolu i Eurojustu, co zapewnia spójność oraz dostosowanie odpowiednich ram prawnych. Przewidziano w nim również zbliżający się przegląd rozporządzenia (UE) 2017/1939 ustanawiającego EPPO[(2)], z uwzględnieniem jego przyszłych zmian i bez uszczerbku dla oceny możliwych wariantów strategicznych dotyczących przeglądu rozporządzenia w sprawie EPPO. To skoordynowane podejście przyczynia się do powstania kompleksowych i spójnych ram przetwarzania danych operacyjnych przez organy i jednostki organizacyjne Unii.

(2) Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej (Dz.U. L 283 z 31.10.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Ochrona osób fizycznych w związku z przetwarzaniem ich danych osobowych jest prawem podstawowym określonym w art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej.

Niniejszy wniosek oparty jest na art. 16 TFUE stanowiącym podstawę prawną do przyjmowania przepisów o ochronie danych. Artykuł ten umożliwia przyjmowanie przepisów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii podczas wykonywania działań wchodzących w zakres zastosowania prawa Unii. Umożliwia on również przyjmowanie przepisów dotyczących swobodnego przepływu danych osobowych, w tym danych osobowych przetwarzanych przez te instytucje, organy i jednostki organizacyjne.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Nie dotyczy.

- **Proporcjonalność**

Nie dotyczy.

- **Wybór instrumentu**

Nie dotyczy.

3. WYNIKI OCEN EX POST, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Oceny ex post/oceny adekwatności obowiązującego prawodawstwa**

W pierwszym sprawozdaniu Komisji ze stosowania rozporządzenia (UE) 2018/1725 z 2022 r. stwierdzono, że ogólnie rzecz biorąc rozporządzenie to funkcjonuje dobrze i jest adekwatne do zakładanych celów. Jednocześnie wskazano potrzebę interwencji ustawodawczej w celu zminimalizowania fragmentacji przepisów o ochronie danych w odniesieniu do instytucji i organów UE przetwarzających operacyjne dane osobowe podczas prowadzenia działań w ramach współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych (rozdział IX rozporządzenia (UE) 2018/1725, „rozdział dotyczący egzekwowania prawa").

- **Konsultacje z zainteresowanymi stronami**

Przeprowadzono ukierunkowane konsultacje z zainteresowanymi stronami ze wszystkimi podmiotami obecnie lub w przyszłości objętymi rozdziałem IX rozporządzenia (UE) 2018/1725 (tj. Europolem, Eurojustem, EPPO, Fronteksem), a także z Europejskim Inspektorem Ochrony Danych, który jest odpowiedzialny za nadzorowanie przestrzegania przepisów.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Nie dotyczy.

- **Ocena skutków**

Nie uznano za stosowne przeprowadzenia oceny skutków niniejszej inicjatywy ze względu na jej ograniczony zakres i w dużej mierze techniczny charakter proponowanych zmian. Wniosek dotyczy przepisów szczegółowych rozporządzenia (UE) 2018/1725 i ma wpływ jedynie na niewielką grupę podmiotów UE w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, bez zmiany ogólnych ram.

Zmiany mają na celu zapewnienie lepiej zharmonizowanego systemu i nie wiążą się z nowymi wariantami strategicznymi; oczekuje się, że będą miały minimalny, niewymierny wpływ na prawa podstawowe i nie będą miały żadnych skutków gospodarczych, społecznych ani środowiskowych. Ponadto odpowiednie agencje są już objęte odrębnymi ewaluacjami i ocenami skutków, w tym dotyczącymi przepisów o ochronie danych, które mają do nich zastosowanie. Odrębna ocena na podstawie rozporządzenia (UE) 2018/1725 powieliłaby to zadanie. Wniosek jest zgodny z wcześniejszym zobowiązaniem Komisji zawartym w jej pierwszym sprawozdaniu ze stosowania rozporządzenia (UE) 2018/1725 z 2022 r., a dalsza ocena rozporządzenia jest planowana na 2027 r. Ponadto nie pojawiają się obawy dotyczące pomocniczości, ponieważ rozporządzenie (UE) 2018/1725 ma zastosowanie wyłącznie do organów UE, których funkcjonowanie nie może być regulowane przez państwa członkowskie.

- **Sprawność regulacyjna i uproszczenie**

Wniosek harmonizuje i upraszcza przepisy o ochronie danych mające zastosowanie do organów i jednostek organizacyjnych Unii działających w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych. Dzięki usprawnieniu obowiązujących przepisów zwiększa on jasność i spójność prawa w obrębie ram instytucjonalnych, ułatwiając tym samym ich stosowanie i zmniejszając złożoność administracyjną. Jakkolwiek korzyści nie są łatwo mierzalne, oczekuje się, że wniosek zmniejszy koszty przestrzegania przepisów i obciążenia administracyjne związane z poruszaniem się pośród różnych lub nakładających się na siebie wymogów. Wniosek wspiera również rozwój wszelkich mechanizmów wymiany między podmiotami rozważanych w kontekście przeglądu struktury zwalczania nadużyć finansowych.

- **Prawa podstawowe**

Ukierunkowany charakter zmian zapewnia utrzymanie obecnego poziomu ochrony danych, a jednocześnie służy poprawie spójności obowiązujących przepisów oraz dalszej harmonizacji.

4. WPŁYW NA BUDŻET

Nie dotyczy.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Nie dotyczy.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Art. 1 obejmuje zmiany w rozporządzeniu (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii.

Pkt 1 zastępuje art. 2 ust. 2 oraz rozszerza zakres stosowania art. 43, 44, 45 i rozdziałów VII i VIII rozporządzenia (UE) 2018/1725 o przetwarzanie operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii, bez uszczerbku dla przepisów szczegółowych o ochronie danych mających zastosowanie do organów i jednostek organizacyjnych Unii. Skreśla się w nim również art. 2 ust. 3, rozszerzając tym samym stosowanie rozporządzenia (UE) 2018/1725 na EPPO, nie podważając jednak potrzeby utrzymania w rozporządzeniu

w sprawie EPPO szczegółowych przepisów o ochronie danych, które uwzględniają odrębny charakter EPPO jako niezależnego organu dochodzeniowo-śledczego i prokuratorskiego Unii.

W pkt 2 wprowadza się dostosowania techniczne w brzmieniu art. 45 dotyczącego zadań inspektora ochrony danych oraz przewiduje, że zadania te będą obejmować również przetwarzanie danych operacyjnych.

W pkt 3 rozszerza się uprawnienie Europejskiego Inspektora Ochrony Danych do nakładania administracyjnych kar pieniężnych przewidziane w art. 66 rozporządzenia (UE) 2018/1725 o przetwarzanie operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii.

W pkt 4 uchyla się art. 70 rozporządzenia (UE) 2018/1725, który jest nieaktualny w świetle przepisów mających zastosowanie do przetwarzania danych operacyjnych, przewidzianych w art. 2 ust. 2.

W pkt 5 zmienia się art. 77 rozporządzenia (UE) 2018/1725 w celu zapewnienia zgodności z wnioskiem dotyczącym aktu zbiorczego prawa cyfrowego oraz zwiększenia pewności prawa poprzez doprecyzowanie, że decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu operacyjnych danych osobowych są dopuszczalne, jeżeli spełnione są szczególne warunki.

W pkt 6 zmienia się art. 78 rozporządzenia (UE) 2018/1725 w celu zapewnienia zgodności z wnioskiem dotyczącym aktu zbiorczego prawa cyfrowego poprzez doprecyzowanie pojęcia żądań stanowiących nadużycie w kontekście prawa dostępu. W szczególności określono w nim, że żądanie można uznać za ewidentnie nieuzasadnione, jeżeli osoba, której dane dotyczą, powołuje się na prawo dostępu do celów innych niż ochrona jej danych. W takich przypadkach administrator może odmówić podjęcia działań w odpowiedzi na żądanie, pozostając jednocześnie zobowiązanym do wykazania, że żądanie jest ewidentnie nieuzasadnione lub nadmierne.

W pkt 7 wprowadza się do rozporządzenia (UE) 2018/1725 nowy art. 87a dotyczący prowadzenia rejestrów operacyjnych danych osobowych, zgodnie z przepisami dyrektywy o ochronie danych w sprawach karnych.

W pkt 8 i 9 wprowadzono dodatkowe zabezpieczenia do art. 88 rozporządzenia (UE) 2018/1725 dotyczącego ewidencji czynności.

W pkt 10 zmienia się art. 92 ust. 1 rozporządzenia (UE) 2018/1725 w celu zapewnienia zgodności z wnioskiem dotyczącym aktu zbiorczego prawa cyfrowego poprzez przedłużenie terminu do zgłoszenia Europejskiemu Inspektorowi Ochrony Danych naruszenia ochrony danych osobowych z 72 do 96 godzin. Podnosi się również próg powodujący obowiązek zgłoszenia, przewidując, że zgłoszenie jest wymagane tylko wtedy, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

Pkt 11 i 12 porządkują ramy prawne regulujące przekazywanie operacyjnych danych osobowych do państw trzecich i organizacji międzynarodowych poprzez dostosowanie ich do ram ustanowionych w dyrektywie (UE) 2016/680. Zmiany te zapewniają jednolity zbiór przepisów mających zastosowanie do organów i jednostek organizacyjnych Unii działających w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych, przy jednoczesnym uwzględnieniu ich szczególnego kontekstu operacyjnego i prawnego, w tym umów o współpracy. Zmienione przepisy przewidują, że przekazywanie danych do państw, w odniesieniu do których wydano decyzję stwierdzającą odpowiedni stopień ochrony, jest dozwolone bez dodatkowego zezwolenia; w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony przekazywanie danych jest dozwolone, jeżeli istnieją

odpowiednie zabezpieczenia w postaci prawnie wiążącego instrumentu lub oceny administratora; a w szczególnych sytuacjach, w których ani nie istnieje decyzja stwierdzająca odpowiedni stopień ochrony, ani nie ma odpowiednich zabezpieczeń, zastosowanie mają pewne odstępstwa. Wreszcie zmienione przepisy przewidują także przekazywanie operacyjnych danych osobowych odbiorcom, którzy nie są właściwymi organami mającymi siedzibę w państwach trzecich, w szczególnych przypadkach, jeżeli spełnione są wymienione w tych przepisach warunki, w tym kiedy skontaktowanie się z właściwym organem w państwie trzecim może być nieskuteczne lub niewłaściwe, oraz jeżeli przekazanie jest bezwzględnie konieczne do wykonywania zadań administratora.

W pkt 13 uporządkowano uprawnienia Europejskiego Inspektora Ochrony Danych w zakresie operacyjnych danych osobowych w odniesieniu do wszystkich organów i jednostek organizacyjnych Unii działających w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych, w zgodzie z uprawnieniami Europejskiego Inspektora Ochrony Danych mających zastosowanie do Europolu od 2022 r.

W art. 2 określono, kiedy nowe przepisy wchodzą w życie.

2026/0173 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

zmieniające Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych.

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 ust. 2,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Ochrona osób fizycznych w zakresie przetwarzania danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Prawo to gwarantuje również art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

(2) Rozporządzenie (UE) 2018/1725 Parlamentu Europejskiego i Rady [(1)] ustanawia ramy prawne przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii. Nadal jednak występuje fragmentaryzacja przepisów o ochronie danych dotyczących przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii podczas wykonywania przez nie czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE – przepisy te znajdują się zarówno w rozdziale IX rozporządzenia (UE) 2018/1725, jak i w innych aktach prawnych Unii. Art. 98 tego rozporządzenia zobowiązuje Komisję do dokonania przeglądu przepisów mających zastosowanie do przetwarzania operacyjnych danych osobowych w celu stwierdzenia ewentualnych niespójności, luk i rozbieżności. Przewidziano w nim również, że Komisja, w stosownych przypadkach, może przedstawić wnioski ustawodawcze w celu wyeliminowania stwierdzonych niedociągnięć, w tym w szczególności w celu rozszerzenia zastosowania rozdziału IX na Prokuraturę Europejską (EPPO) ustanowioną rozporządzeniem Rady (UE) 2017/1939 [(2)], w razie potrzeby, oraz w celu wprowadzenia modyfikacji tego

[(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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

[(2)] Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej (Dz.U. L 283 z 31.10.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

rozdziału. W pierwszym sprawozdaniu ze stosowania rozporządzenia (UE) 2018/1725 Komisja potwierdziła ogólną skuteczność rozporządzenia w zapewnianiu wysokiego poziomu ochrony danych osobowych, podkreślając jednocześnie szereg niespójności, rozbieżności i fragmentacji prawnej wynikających ze wzajemnych zależności między rozdziałem IX a innymi przepisami rozporządzenia (UE) 2018/1725, a także istnienia odrębnego systemu ochrony danych dotyczącego EPPO.

(3) Obecnie do przetwarzania operacyjnych danych osobowych zastosowanie mają wyłącznie art. 3 i rozdział IX rozporządzenia (UE) 2018/1725, wraz z szeregiem szczegółowych przepisów o ochronie danych określonych w aktach ustanawiających Agencję Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) i Agencję Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust). Jednocześnie w akcie ustanawiającym Prokuraturę Europejską przewidziano jej własny, niezależny system ochrony danych. Należy zatem zmienić rozporządzenie (UE) 2018/1725, aby rozszerzyć stosowanie jego rozdziału IX na wszystkie organy i jednostki organizacyjne Unii przetwarzające operacyjne dane osobowe w sektorze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych, zaprowadzić pewność prawa poprzez wyeliminowanie luk w obecnym systemie ochrony danych, w szczególności w odniesieniu do Europejskiej Agencji Straży Granicznej i Przybrzeżnej, oraz uporządkować przepisy dotyczące międzynarodowego przekazywania danych osobowych, a także przepisy dotyczące uprawnień Europejskiego Inspektora Ochrony Danych. Zmiany te nie powinny mieć wpływu na możliwość utrzymania w rozporządzeniu (UE) 2017/1939 szczegółowych przepisów o ochronie danych niezbędnych do uwzględnienia wyjątkowego charakteru Prokuratury Europejskiej jako niezależnej prokuratury Unii.

(4) Aby stworzyć zharmonizowane, spójne, uproszczone i kompletne ramy prawne przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii, definicje (rozdział I), przepisy dotyczące inspektorów ochrony danych (rozdział IV sekcja 6), przepisy dotyczące współpracy i spójności (rozdział VII), przepisy dotyczące środków ochrony prawnej, odpowiedzialności i sankcji (rozdział VIII) oraz przepisy dotyczące przetwarzania operacyjnych danych osobowych (które należy dostosować do przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 [3] – rozdział IX) ustanowione w rozporządzeniu (UE) 2018/1725 powinny mieć zastosowanie do organów i jednostek organizacyjnych Unii podczas wykonywania czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE. Przepisy te powinny mieć zastosowanie w przypadku gdy wykonują one takie czynności w celach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania przestępstw. Przepisy te, a nie tylko rozdział IX rozporządzenia (UE) 2018/1725, powinny mieć również zastosowanie do przetwarzania operacyjnych danych osobowych przez Europejską Agencję Straży Granicznej i Przybrzeżnej. Przepisy rozporządzenia (UE) 2018/1725 powinny mieć zastosowanie bez naruszenia przepisów szczegółowych mających zastosowanie do przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii podczas wykonywania czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, w szczególności

[3] Dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

przepisów określonych w aktach ustanawiających Europol, Eurojust i EPPO. Takie przepisy szczegółowe należy uznać za *lex specialis* w stosunku do przepisów rozporządzenia (UE) 2018/1725 dotyczących przetwarzania operacyjnych danych osobowych.

(5) Inspektor ochrony danych we wszystkich instytucjach i organach Unii powinien zapewnić stosowanie wszystkich przepisów o ochronie danych, w tym rozporządzenia (UE) 2018/1725. Inspektorzy powinni również doradzać administratorom i podmiotom przetwarzającym w kwestii ich obowiązków. Aby zapewnić spójność i zapobiec powielaniu działań w sprawach dotyczących zarówno administracyjnych, jak i operacyjnych danych osobowych, powinien istnieć tylko jeden zbiór przepisów dotyczących inspektorów ochrony danych.

(6) Europejski Inspektor Ochrony Danych powinien być uprawniony do nakładania administracyjnych kar pieniężnych jako środka ostatecznego, między innymi za przetwarzanie operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii działające w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych.

(7) Aby uniknąć powielania działań w ramach rozporządzenia (UE) 2018/1725, należy uchylić jego art. 70, ponieważ zakres rozdziału IX jest już uregulowany w art. 2 rozporządzenia (UE) 2018/1725.

(8) Aby zapewnić dostosowanie do rozporządzenia (UE) …/… [*wniosek dotyczący aktu zbiorczego prawa cyfrowego*], w art. 77 rozporządzenia (UE) 2018/1725 należy doprecyzować, że decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu operacyjnych danych osobowych są dozwolone, jeżeli spełnione są określone warunki.

(9) Aby zapewnić dostosowanie do rozporządzenia (UE) …/… [*wniosek dotyczący aktu zbiorczego prawa cyfrowego*], w art. 78 rozporządzenia (UE) 2018/1725 należy doprecyzować, że prawa dostępu, które z założenia jest korzystne dla osób, których dane dotyczą, nie należy nadużywać w rozumieniu nadużywania go przez osoby, których dane dotyczą, do innych celów niż ochrona ich danych.

(10) Aby wykazać zgodność z rozporządzeniem (UE) 2018/1725, organy i jednostki organizacyjne Unii działające w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych powinny mieć jednolite przepisy dotyczące prowadzenia rejestrów wszystkich kategorii czynności przetwarzania, za które są odpowiedzialne. Każdy administrator i podmiot przetwarzający powinien być zobowiązany do współpracy z Europejskim Inspektorem Ochrony Danych i na jego wniosek powinien udostępniać mu swoje rejestry w celu monitorowania wspomnianych operacji przetwarzania.

(11) Organy i jednostki organizacyjne Unii nie powinny mieć możliwości modyfikowania ewidencji. W przypadku gdy organy i jednostki organizacyjne Unii otrzymują operacyjne dane osobowe od właściwych organów krajowych, organy i jednostki organizacyjne Unii powinny przekazywać ewidencję tym organom, jeżeli jest ona niezbędna do wewnętrznych dochodzeń dotyczących zgodności z przepisami w zakresie ochrony danych.

(12) Aby zapewnić dostosowanie do rozporządzenia (UE) …/… [*wniosek dotyczący aktu zbiorczego prawa cyfrowego*], próg powinien być wyższy, a termin do zgłoszenia naruszenia ochrony danych osobowych Europejskiemu Inspektorowi Ochrony Danych należy przedłużyć.

(13) Wszystkie organy i jednostki organizacyjne Unii działające w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych powinny korzystać z jednolitego zbioru przepisów dotyczących międzynarodowego przekazywania operacyjnych danych osobowych, dostosowanego do dyrektywy (UE) 2016/680.

(14) Zgodnie z art. 36 dyrektywy (UE) 2016/680 Komisja może stwierdzić, że państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizacja międzynarodowa zapewnia odpowiedni stopień ochrony danych. W takich przypadkach przekazywanie operacyjnych danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej przez organy lub jednostki organizacyjne Unii może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia.

(15) Przekazania nieprzeprowadzone na podstawie decyzji stwierdzającej odpowiedni stopień ochrony powinny być dopuszczalne jedynie wtedy, gdy w prawnie wiążącym akcie przewidziano odpowiednie zabezpieczenia zapewniające ochronę danych osobowych, lub gdy administrator ocenił wszystkie okoliczności towarzyszące przekazaniu danych i na podstawie tej oceny stwierdza, że istnieją odpowiednie zabezpieczenia w odniesieniu do ochrony danych osobowych. Takimi prawnie wiążącymi aktami mogą być na przykład umowy o współpracy między Eurojustem a państwem trzecim zawarte przed dniem 12 grudnia 2019 r. zgodnie z art. 26a decyzji 2002/187/WSiSW, umowy o współpracy między Europolem a państwem trzecim zawarte przed dniem 1 maja 2017 r. zgodnie z art. 23 decyzji 2009/371/WSiSW lub umowy międzynarodowe zawarte między Unią a państwem trzecim zgodnie z art. 218 TFUE.

(16) W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń przekazanie lub kategoria przekazań mogą mieć miejsce w drodze odstępstwa w szczególnych sytuacjach. Wyjątki należy interpretować w sposób zawężający i nie powinny one umożliwiać częstego, masowego i zorganizowanego przekazywania danych osobowych ani przekazywania danych na dużą skalę; powinny też być ograniczone do danych ściśle niezbędnych. Takie operacje przekazywania powinny być udokumentowane, a dokumentacja ta powinna być udostępniana na wniosek Europejskiemu Inspektorowi Ochrony Danych w celu kontroli zgodności przekazania z prawem.

(17) W konkretnych indywidualnych przypadkach rutynowy tryb postępowania wymagający skontaktowania się z właściwym organem w państwie trzecim może okazać się nieskuteczny lub niewłaściwy, w szczególności ze względu na to, że przekazanie mogłoby ulec opóźnieniu, lub dlatego, że organ w państwie trzecim nie przestrzega praworządności lub międzynarodowych norm i standardów ochrony praw człowieka. Może się tak zdarzyć wówczas, gdy zachodzi pilna potrzeba przekazania danych osobowych spółce prywatnej w państwie trzecim w celu uzyskania informacji o nieznanym sprawcy przestępstwa internetowego, w celu ratowania życia osobie zagrożonej czynem zabronionym lub gdy jest to konieczne do zapobieżenia spodziewanemu popełnieniu czynu zabronionego, w tym czynu o charakterze terrorystycznym. W takich przypadkach, przy zachowaniu szczególnych warunków, organy i jednostki organizacyjne Unii mogą podjąć decyzję o przekazaniu operacyjnych danych osobowych bezpośrednio odbiorcom, którzy nie są właściwymi organami, mającym siedzibę w tych państwach trzecich.

(18) Europejski Inspektor Ochrony Danych powinien dysponować jednolitym zestawem uprawnień mających zastosowanie do przetwarzania operacyjnych danych osobowych

przez organy i jednostki organizacyjne Unii działające w obszarze ścigania przestępstw i wymiaru sprawiedliwości w sprawach karnych. Takie uprawnienia, na przykład do nakazania administratorowi danych zapewnienia zgodności z rozporządzeniem (UE) 2018/1725, nakazania zawieszenia przepływu danych do odbiorcy w państwie członkowskim, państwie trzecim lub organizacji międzynarodowej lub nałożenia administracyjnej kary pieniężnej w przypadku niezastosowania się do nakazu, mają już zastosowanie do Europolu od 2022 r.

(19) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia XX XX 2026 r.,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Zmiany w **rozporządzeniu (UE) 2018/1725**

W rozporządzeniu (UE) 2018/1725 wprowadza się następujące zmiany:

1. w art. 2 wprowadza się następujące zmiany:

   a) ust. 2 otrzymuje brzmienie:

   „2. Do przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii prowadzące czynności, które wchodzą w zakres stosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, stosuje się jedynie art. 3, 43, 44, 45 oraz rozdziały VII, VIII i IX niniejszego rozporządzenia, nie naruszając szczegółowych przepisów dotyczących ochrony danych mających zastosowanie do takich organów lub jednostek organizacyjnych Unii.”;

   b) uchyla się ust. 3;

2. art. 45 ust. 1 lit. d), e) i f) otrzymują brzmienie:

   „d) udzielanie na żądanie porad co do konieczności zgłoszenia lub zawiadomienia o naruszeniu ochrony danych osobowych na podstawie przepisów art. 34 i 35 lub art. 92 i 93;

   e) udzielanie na żądanie porad co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania na podstawie art. 39 lub 89, a także konsultowanie się z Europejskim Inspektorem Ochrony Danych w razie wątpliwości co do konieczności wykonania oceny skutków dla ochrony danych;

   f) udzielanie na żądanie porad co do konieczności przeprowadzenia uprzednich konsultacji z Europejskim Inspektorem Ochrony Danych na podstawie art. 40 lub art. 90; konsultowanie się z Europejskim Inspektorem Ochrony Danych w razie wątpliwości co do konieczności uprzednich konsultacji;”;

3. w art. 66 ust. 1 zdanie pierwsze otrzymuje brzmienie:

   „1. Europejski Inspektor Ochrony Danych może nakładać administracyjne kary pieniężne na instytucje i organy Unii – w zależności od okoliczności w poszczególnych przypadkach – w sytuacji gdy instytucja lub organ Unii nie zastosują się do poleceń Europejskiego Inspektora Ochrony Danych na podstawie art. 58 ust. 2 lit. d)–h) i j) lub na podstawie art. 95a ust. 3 lit. c), e), f), j) i k).”;

4. uchyla się art. 70 rozporządzenia;

5. art. 77 ust. 1 otrzymuje brzmienie:

„1. Decyzja, która wywołuje skutki prawne dla osoby, której dane dotyczą, lub w podobny sposób znacząco na nią wpływa, może opierać się wyłącznie na zautomatyzowanym przetwarzaniu, w tym również na profilowaniu tylko wtedy, gdy taką decyzję dopuszcza prawo Unii, któremu podlega administrator i które przewiduje również odpowiednie środki zabezpieczenia praw i wolności osoby, której dane dotyczą, przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora.”;

6. art. 78 ust. 4 otrzymuje brzmienie:

„4. Administrator zapewnia, aby informacje przekazywane na mocy art. 79 oraz wszelka komunikacja i wszelkie działania podjęte na mocy art. 80–84 i 92 były wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, lub w przypadku żądań na podstawie art. 80, gdy osoba, której dane dotyczą, nadużywa prawa dostępu do celów innych niż ochrona jej danych, administrator może odmówić podjęcia żądanych działań. Na administratorze spoczywa obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony charakter lub że istnieją uzasadnione podstawy, by sądzić, że jest on nadmierny.”;

7. dodaje się art. 87a w brzmieniu:

„Artykuł 87a

Rejestry kategorii czynności przetwarzania operacyjnych danych osobowych

1. Każdy administrator prowadzi rejestr wszystkich kategorii czynności przetwarzania operacyjnych danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się wszystkie następujące informacje:

a) dane kontaktowe administratora oraz imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych, a także w stosownych przypadkach – dane kontaktowe współadministratora;

b) cele przetwarzania;

c) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym podmiotów prywatnych, oraz odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

d) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

e) w stosownym przypadku informacje o stosowaniu profilowania;

f) w stosownym przypadku kategorie przekazań danych osobowych do podmiotu prywatnego, państwa trzeciego lub organizacji międzynarodowej;

g) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;

h) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

i) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 91 ust. 1.

2. Podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora zawierający następujące informacje:

a) dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających każdego administratora, w imieniu którego działa podmiot przetwarzający, a także dane kontaktowe inspektora ochrony danych;

b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

c) w stosownym przypadku przypadki przekazania danych osobowych do podmiotu prywatnego, państwa trzeciego lub organizacji międzynarodowej, w razie jednoznacznego polecenia administratora, łącznie z nazwą tego państwa trzeciego lub organizacji międzynarodowej;

d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 91 ust. 1.

3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną. Administrator i podmiot przetwarzający udostępniają te rejestry Europejskiemu Inspektorowi Ochrony Danych na jego wniosek.”;

8. w art. 88 ust. 1 dodaje się zdanie w brzmieniu:

„Nie ma możliwości modyfikowania ewidencji.”;

9. w art. 88 ust. 3 dodaje się zdanie w brzmieniu:

„Jeżeli wymaga tego właściwy organ krajowy do celów konkretnego dochodzenia związanego z przestrzeganiem przepisów o ochronie danych, ewidencję, o której mowa w ust. 1, przekazuje się temu organowi.”;

10. art. 92 ust. 1 otrzymuje brzmienie:

„1. W przypadku naruszenia ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 96 godzin po stwierdzeniu tego naruszenia – zgłasza je Europejskiemu Inspektorowi Ochrony Danych. Do zgłoszenia, które przekazano Europejskiemu Inspektorowi Ochrony Danych po upływie 96 godzin, dołącza się wyjaśnienie przyczyn opóźnienia.”;

11. art. 94 otrzymuje brzmienie:

„Artykuł 94

Zasady ogólne dotyczące przekazywania operacyjnych danych osobowych do państw trzecich i organizacji międzynarodowych

1. Administrator może przekazywać operacyjne dane osobowe do państwa trzeciego lub do organizacji międzynarodowej – z zastrzeżeniem przestrzegania mających zastosowanie przepisów dotyczących ochrony danych i innych przepisów niniejszego rozporządzenia – tylko wtedy, gdy spełnione są następujące warunki:

a) przekazanie jest niezbędne do wykonywania przez administratora jego zadań;

b) organ państwa trzeciego lub organizacja międzynarodowa, którym przekazywane są dane operacyjne, są właściwe w zakresie ścigania przestępstw lub wymiaru sprawiedliwości w sprawach karnych;

c) w przypadku gdy operacyjne dane osobowe będące przedmiotem przekazania zostały przekazane lub udostępnione administratorowi przez państwo

członkowskie bądź organ lub jednostkę organizacyjną Unii, administrator uzyskuje uprzednią zgodę na przekazanie od odpowiedniego właściwego organu tego państwa członkowskiego lub od organu lub jednostki organizacyjnej Unii zgodnie z mającym zastosowanie prawem państwa członkowskiego lub prawem Unii, chyba że to państwo członkowskie bądź ten organ lub jednostka organizacyjna Unii zezwoliły na takie przekazanie na warunkach ogólnych lub z zastrzeżeniem szczególnych warunków;

d) w przypadku dalszego przekazania danych przez państwo trzecie lub organizację międzynarodową do innego państwa trzeciego lub organizacji międzynarodowej administrator wymaga od przekazującego państwa trzeciego lub przekazującej organizacji międzynarodowej uzyskania uprzedniej zgody administratora na to dalsze przekazanie;

e) Administrator może udzielić zgody na mocy lit. d) wyłącznie po uzyskaniu uprzedniej zgody państwa członkowskiego bądź organu lub jednostki organizacyjnej Unii, od którego lub której dane pochodzą, w stosownych przypadkach, po należytym uwzględnieniu wszystkich istotnych czynników, w tym wagi przestępstwa, celu, w jakim operacyjne dane osobowe zostały pierwotnie przekazane, oraz stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których operacyjne dane osobowe mają zostać dalej przekazane.

2. Z zastrzeżeniem warunków określonych w ust. 1 niniejszego artykułu administrator może przekazać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej, jeżeli spełnione są warunki określone w art. 94a, 94b, 94c lub 94d.

3. Nie naruszając art. 94c, administrator może przekazywać operacyjne dane osobowe właściwemu organowi państwa uczestniczącego we wdrażaniu, stosowaniu i rozwijaniu dorobku Schengen, które wdrożyło i skutecznie stosuje przepisy dyrektywy (UE) 2016/680 oraz przepisy dotyczące wymiany informacji określone w dyrektywie (UE) 2023/977.

4. W pilnych przypadkach administrator może przekazać operacyjne dane osobowe bez uprzedniej zgody państwa członkowskiego bądź organu lub jednostki organizacyjnej Unii zgodnie z ust. 1 lit. c). Administrator może tego dokonać wyłącznie wtedy, gdy przekazanie operacyjnych danych osobowych jest niezbędne do zapobieżenia bezpośredniemu i poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego lub gdy jest ono niezbędne do ważnych interesów państwa członkowskiego, a uprzedniej zgody nie da się uzyskać w odpowiednim terminie. Organ odpowiadający za wydanie uprzedniej zgody zostaje powiadomiony niezwłocznie.

5. Wszystkie przepisy niniejszego rozdziału dotyczące przekazań międzynarodowych stosuje się w celu zapewnienia, by stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu nie został obniżony.”;

12. dodaje się artykuły w brzmieniu:

„Artykuł 94a

Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony

Administrator może przekazywać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej, jeżeli Komisja zgodnie z art. 36 dyrektywy (UE)

2016/680 stwierdzi, że to państwo trzecie, terytorium lub co najmniej jeden określony sektor w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

Artykuł 94b

Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń

1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony administrator może przekazywać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej, jeżeli:

a) w prawnie wiążącym akcie przewidziano odpowiednie zabezpieczenia ochrony operacyjnych danych osobowych;

b) lub administrator ocenił wszystkie okoliczności związane z przekazaniem operacyjnych danych osobowych i stwierdził, że istnieją odpowiednie zabezpieczenia ochrony operacyjnych danych osobowych.

2. Prawnie wiążącym aktem, o którym mowa w ust. 1 lit. a), jest:

a) umowa międzynarodowa między Unią a danym państwem trzecim lub organizacją międzynarodową zgodnie z art. 218 TFUE, która przewiduje odpowiednie zabezpieczenia w odniesieniu do ochrony prywatności, ochrony danych oraz innych podstawowych praw i wolności osób fizycznych;

b) przed dniem 12 grudnia 2019 r. zawarto umowę o współpracy umożliwiającą wymianę operacyjnych danych osobowych między Eurojustem a tym państwem trzecim lub organizacją międzynarodową zgodnie z art. 26a decyzji 2002/187/WSiSW; lub

c) umowę o współpracy umożliwiającą wymianę operacyjnych danych osobowych zawartą przed dniem 1 maja 2017 r. między Europolem a danym państwem trzecim lub daną organizacją międzynarodową zgodnie z art. 23 decyzji 2009/371/WSiSW.

3. Organy i jednostki organizacyjne Unii mogą zawierać porozumienia robocze w celu określenia warunków wykonywania umów, o których mowa w ust. 2.

4. Administrator informuje Europejskiego Inspektora Ochrony Danych o kategoriach przekazań na podstawie ust. 1 lit. b).

5. Jeżeli przekazanie odbywa się na podstawie ust. 1 lit. b), musi być ono udokumentowane, a dokumentację udostępnia się Europejskiemu Inspektorowi Ochrony Danych na jego wniosek. Dokumentacja obejmuje zapis daty i godziny przekazania oraz informacje o właściwym organie odbierającym, o uzasadnieniu przekazania oraz o przekazanych operacyjnych danych osobowych

Artykuł 94c

Wyjątki w szczególnych sytuacjach

1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń określonych w art. 94b administrator może przekazać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie pod warunkiem, że przekazanie ich jest niezbędne:

a) w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby;

b) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą;

c) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego;

d) lub w indywidualnych przypadkach w celu wykonania zadań administratora, chyba że stwierdzi on, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem.

2. Jeżeli przekazanie odbywa się na podstawie ust. 1, musi być ono udokumentowane, a dokumentację udostępnia się Europejskiemu Inspektorowi Ochrony Danych na jego wniosek. Dokumentacja obejmuje zapis daty i godziny przekazania oraz informacje o właściwym organie odbierającym, o uzasadnieniu przekazania oraz o przekazanych operacyjnych danych osobowych.

Artykuł 94d

Przekazywanie operacyjnych danych osobowych odbiorcom mającym siedzibę w państwach trzecich

1. W drodze odstępstwa od art. 94 ust. 1 lit. b) i nie naruszając umów międzynarodowych, o których mowa w ust. 2 niniejszego artykułu, administrator może w indywidualnych, konkretnych przypadkach przekazywać operacyjne dane osobowe bezpośrednio odbiorcom mającym siedzibę w państwach trzecich jedynie wówczas, gdy spełnione zostały wszystkie następujące warunki:

a) przekazanie jest bezwzględnie konieczne do wykonywania zadań administratora, do celów których dozwolone jest przetwarzanie operacyjnych danych osobowych;

b) administrator stwierdzi, że podstawowe prawa i wolności danej osoby, której dane dotyczą, nie są nadrzędne wobec interesu publicznego przemawiającego za przedmiotowym przekazaniem;

c) administrator uzna, że przekazanie właściwemu organowi w państwie trzecim byłoby nieskuteczne lub niewłaściwe, w szczególności dlatego, że przekazanie nie może nastąpić w odpowiednim terminie;

d) właściwy organ w państwie trzecim zostanie niezwłocznie poinformowany, chyba że jest to nieskuteczne lub niewłaściwe;

e) administrator poinformuje odbiorcę o konkretnym celu lub konkretnych celach, w których operacyjne dane osobowe mają być wyłącznie przetwarzane przez odbiorcę, pod warunkiem że takie przetwarzanie jest niezbędne.

2. Umowa międzynarodowa, o której mowa w ust. 1, oznacza dwustronną lub wielostronną umowę międzynarodową obowiązującą między Unią a państwami trzecimi dotyczącą współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

3. Jeżeli przekazanie odbywa się na podstawie ust. 1, musi być ono udokumentowane, a dokumentację, w tym datę i godzinę przekazania, oraz informacje o właściwym organie odbierającym, o uzasadnieniu przekazania oraz o przekazanych operacyjnych danych osobowych należy udostępnić Europejskiemu Inspektorowi Ochrony Danych na jego wniosek.”;

13. dodaje się art. 95a w brzmieniu:

„Artykuł 95a

Nadzór ze strony Europejskiego Inspektora Ochrony Danych

1. Europejski Inspektor Ochrony Danych jest odpowiedzialny za monitorowanie i zapewnienie stosowania przepisów dotyczących ochrony podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii, a także za doradzanie im oraz osobom, których dane dotyczą, we wszystkich kwestiach związanych z przetwarzaniem operacyjnych danych osobowych. W tym celu wypełnia obowiązki określone w ust. 2 i wykonuje uprawnienia określone w ust. 3, ściśle współpracując z krajowymi organami nadzoru.

2. Europejskiemu Inspektorowi Ochrony Danych przysługują następujące uprawnienia:

a) przyjmuje skargi i bada je oraz informuje osobę, której dane dotyczą, o wyniku w rozsądnym terminie; przeprowadza postępowania wyjaśniające z własnej inicjatywy lub na podstawie skarg oraz informuje osoby, których dane dotyczą, o ich wyniku w rozsądnym terminie;

b) monitoruje i zapewnia stosowanie niniejszego rozporządzenia i wszelkich innych aktów Unii dotyczących ochrony osób fizycznych w związku z przetwarzaniem operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii;

c) doradza organom i jednostkom organizacyjnym Unii, albo z własnej inicjatywy, albo w odpowiedzi na konsultacje, we wszystkich kwestiach dotyczących przetwarzania operacyjnych danych osobowych, w szczególności zanim przyjmą przepisy wewnętrzne związane z ochroną podstawowych praw i wolności w odniesieniu do przetwarzania operacyjnych danych osobowych;

d) prowadzi rejestr nowych rodzajów operacji przetwarzania, które mu zgłoszono;

e) przeprowadza uprzednie konsultacje dotyczące przetwarzania, które mu zgłoszono.

3. Na podstawie niniejszego rozporządzenia Europejski Inspektor Ochrony Danych może:

a) doradzać osobom, których dane dotyczą, w kwestii korzystania z ich praw;

b) przekazać sprawę organowi lub jednostce organizacyjnej Unii w przypadku domniemanego naruszenia przepisów regulujących przetwarzanie operacyjnych danych osobowych i w stosownych przypadkach zaproponować środki prawne służące usunięciu tego naruszenia i poprawie ochrony osób, których dane dotyczą;

c) nakazać uwzględnienie żądań skorzystania z niektórych praw w odniesieniu do operacyjnych danych osobowych, jeżeli takie żądania zostały odrzucone z naruszeniem mających zastosowanie przepisów dotyczących praw osób, których dane dotyczą;

d) ostrzegać lub upominać organ lub jednostkę organizacyjną Unii;

e) nakazać organowi lub jednostce organizacyjnej Unii sprostowanie, ograniczenie, usunięcie lub zniszczenie danych osobowych, które zostały przetworzone z naruszeniem przepisów regulujących przetwarzanie operacyjnych danych osobowych, oraz powiadomienie o takich działaniach osób trzecich, którym takie dane zostały ujawnione;

f) nałożyć czasowy lub ostateczny zakaz prowadzenia przez organ lub jednostkę organizacyjną Unii operacji przetwarzania, które naruszają przepisy regulujące przetwarzanie operacyjnych danych osobowych;

g) przekazać sprawę administratorowi lub podmiotowi przetwarzającemu, a w razie konieczności Parlamentowi Europejskiemu, Radzie i Komisji;

h) przekazać sprawę Trybunałowi Sprawiedliwości Unii Europejskiej na warunkach przewidzianych w TFUE;

i) interweniować w sprawach wniesionych do Trybunału Sprawiedliwości Unii Europejskiej;

j) nakazać administratorowi lub podmiotowi przetwarzającemu zapewnienie zgodności operacji przetwarzania z przepisami niniejszego rozporządzenia oraz, w stosownych przypadkach, z przepisami o ochronie danych określonymi w akcie ustanawiającym odpowiedni organ lub jednostkę organizacyjną Unii, w stosownych przypadkach, w określony sposób i w określonym terminie;

k) nakazać zawieszenie przepływu danych do odbiorcy w państwie członkowskim, państwie trzecim lub organizacji międzynarodowej;

l) nałożyć administracyjną karę pieniężną na podstawie art. 66 w razie niewykonania przez organ lub jednostkę organizacyjną Unii co najmniej jednego ze środków, o których mowa w lit. c), e), f), j) i k) niniejszego ustępu, zależnie od okoliczności konkretnej sprawy.

4. Europejski inspektor ochrony danych ma uprawnienia do:

a) uzyskania od organu lub jednostki organizacyjnej Unii dostępu do wszystkich operacyjnych danych osobowych oraz do wszystkich informacji niezbędnych do prowadzonych przez niego dochodzeń;

b) uzyskania dostępu do wszelkich pomieszczeń, w których organ lub jednostka organizacyjna Unii wykonuje czynności, jeżeli są uzasadnione powody, aby przypuszczać, że wykonywana jest tam czynność podlegająca przepisom niniejszego rozdziału.

5. Europejski Inspektor Ochrony Danych przygotowuje roczne sprawozdanie ze swoich działań nadzorczych prowadzonych w odniesieniu do administratorów na podstawie niniejszego rozdziału. Sprawozdanie to stanowi część rocznego sprawozdania Europejskiego Inspektora Ochrony Danych, o którym mowa w art. 60.

EIOD zaprasza krajowe organy nadzoru do przedstawienia uwag na temat tej części rocznego sprawozdania, zanim zostanie on przyjęty. EIOD w największym możliwym stopniu uwzględnia te uwagi i odnosi się do nich w sprawozdaniu rocznym.

Część rocznego sprawozdania, o którym mowa w akapicie drugim, zawiera informacje statystyczne dotyczące skarg, postępowań wyjaśniających i postępowań przygotowawczych, a także dotyczące przekazań operacyjnych danych osobowych państwom trzecim i organizacjom międzynarodowym, przypadków uprzednich konsultacji z Europejskim Inspektorem Ochrony Danych oraz wykorzystania uprawnień określonych w ust. 3 niniejszego artykułu.

6. Europejski Inspektor Ochrony Danych, urzędnicy i inni pracownicy sekretariatu Europejskiego Inspektora Ochrony Danych są zobowiązani do zachowania poufności zgodnie z art. 95.”.

Artykuł 2

Wejście w życie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie ma jednak zastosowanie do przetwarzania operacyjnych danych osobowych przez Prokuraturę Europejską od dnia [*data rozpoczęcia stosowania nowego rozporządzenia w sprawie EPPO*].

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
[...]	*[...]*