OCHRONA DANYCH OSOBOWYCH

Ochrona danych osobowych i poszanowanie życia prywatnego to prawa podstawowe możliwe do wyegzekwowania na drodze prawnej, których nie można rozważać w kontekście interesów handlowych lub politycznych. Parlament Europejski zawsze podkreślał potrzebę utrzymania równowagi między podnoszeniem poziomu bezpieczeństwa i zagwarantowaniem przestrzegania praw człowieka, w tym ochrony danych i prywatności. Nowe przepisy dotyczące ochrony danych w UE wzmacniające prawa obywateli i upraszczające przepisy dla przedsiębiorstw w erze cyfrowej weszły w życie w maju 2018 r.

PODSTAWA PRAWNA

Artykuł 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE);

Artykuł 7 i 8 Karty praw podstawowych Unii Europejskiej.

CELE

Unia musi dopilnować, by podstawowe prawo do ochrony danych, przewidziane w Karcie praw podstawowych Unii Europejskiej, było konsekwentnie przestrzegane. W świetle gwałtownego wzrostu wolumenu przekazywanych danych, przy czym największy udział w tym wzroście mają UE, USA i Kanada, należy wzmocnić stanowisko UE w sprawie ochrony danych osobowych w kontekście wszystkich polityk UE.

OSIĄGNIĘCIA

A. Ramy instytucjonalne

1. Traktat z Lizbony

Przed wejściem w życie traktatu z Lizbony prawodawstwo dotyczące ochrony danych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości było podzielone pomiędzy pierwszy filar (ochrona danych do celów prywatnych i handlowych – z wykorzystaniem metody wspólnotowej) i trzeci filar (ochrona danych do celów egzekwowania prawa – na poziomie międzyrządowym). W związku z tym proces decyzyjny odbywał się w tych dwóch obszarach w oparciu o odmienne reguły. Struktura filarowa przestała obowiązywać w chwili wejścia w życie traktatu z Lizbony, który stanowi solidniejszą podstawę rozwoju bardziej przejrzystego i skutecznego systemu ochrony danych i który przewiduje jednocześnie przyznanie nowych kompetencji Parlamentowi, nadając mu status współprawodawcy. Artykuł 16 TFUE stanowi, że Parlament i Rada określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy, biura i agencje Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres stosowania prawa Unii.

2. Strategiczne wytyczne dla przestrzeni wolności, bezpieczeństwa i sprawiedliwości

W następstwie programu z Tampere i programu haskiego (odpowiednio z października 1999 r. i listopada 2004 r.) Rada Europejska zatwierdziła w grudniu 2009 r. wieloletni program dotyczący przestrzeni wolności, bezpieczeństwa i sprawiedliwości na lata 2010–2014, nazywany programem sztokholmskim. W konkluzjach ze szczytu w czerwcu 2014 r. Rada Europejska określiła strategiczne wytyczne planowania ustawodawczego i operacyjnego na nadchodzące lata w ramach programu dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości, zgodnie z art. 68 TFUE. Jednym z głównych celów jest lepsza ochrona danych osobowych w UE.

B. Najważniejsze instrumenty prawne w zakresie ochrony danych

1. Karta praw podstawowych UE

Art. 7 i 8 Karty praw podstawowych Unii Europejskiej uznają poszanowanie życia prywatnego oraz ochronę danych osobowych za blisko ze sobą powiązane, jednak odrębne prawa podstawowe.

2. Rada Europy

a. Konwencja 108 z 1981 r.

Konwencja 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych była pierwszym prawnie wiążącym instrumentem międzynarodowym przyjętym w dziedzinie ochrony danych. Ma ona na celu zagwarantowanie każdej osobie fizycznej „poszanowania jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych". Protokół zmieniający konwencję ma na celu poszerzenie jej zakresu, zwiększenie poziomu ochrony danych i poprawę jej skuteczności.

b. Europejska konwencja praw człowieka

W art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r. zapisano prawo każdej osoby do poszanowania życia prywatnego i rodzinnego, domu i korespondencji.

3. Aktualnie obowiązujące instrumenty prawne UE w zakresie ochrony danych

a. Ogólne rozporządzenie o ochronie danych

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 (ogólne rozporządzenie o ochronie danych) zaczęło obowiązywać w maju 2018 r. Przepisy te mają na celu ochronę wszystkich obywateli UE przed naruszaniem prywatności i ochrony danych w świecie coraz bardziej opartym na danych, przy jednoczesnym stworzeniu bardziej przejrzystych i spójnych ram dla przedsiębiorstw. Prawa, które przysługują obywatelom, obejmują wymóg wyraźnej zgody na przetwarzanie ich danych oraz prawo do uzyskania jasnych i zrozumiałych informacji na ten temat; prawo do bycia zapomnianym: obywatel może zwrócić się o wykasowanie jego danych; prawo do przeniesienia danych do innego usługodawcy (np. w przypadku zmiany sieci społecznościowej na inną); oraz prawo

do otrzymania informacji w przypadku złamania zabezpieczeń danych. Nowe przepisy mają zastosowanie do wszystkich przedsiębiorstw działających w UE, nawet jeśli mają one siedzibę poza Unią. Ponadto w przypadku przedsiębiorstw naruszających przepisy można zastosować środki naprawcze, takie jak ostrzeżenia i nakazy lub kary finansowe.

W dniu 25 lipca 2024 r. Komisja Europejska przedstawiła drugie sprawozdanie w sprawie stosowania ogólnego rozporządzenia o ochronie danych. 16 lipca 2025 r. Komisja zorganizowała w Brukseli dialog na temat stosowania rozporządzenia o ochronie danych (RODO). Dialog ten był następstwem inicjatyw takich jak wniosek zbiorczy Komisji w sprawie zwolnienia podmiotów zatrudniających mniej niż 750 pracowników z obowiązku prowadzenia dokumentacji na podstawie RODO.

W 2023 r. Komisja zaproponowała nowe rozporządzenie w sprawie przepisów proceduralnych RODO, którego celem jest usprawnienie współpracy między organami ochrony danych przy egzekwowaniu RODO w sprawach transgranicznych. Ustanowiono w nim przepisy proceduralne, których organy ochrony danych muszą przestrzegać podczas stosowania RODO w sprawach dotyczących osób fizycznych w więcej niż jednym państwie członkowskim. W dniu 21 października 2025 r. Parlament zatwierdził nowe przepisy mające przyspieszyć transgraniczne egzekwowanie RODO, wyjaśniając tym samym odpowiednie procedury i prawa.

b. Dyrektywa w sprawie egzekwowania prawa

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 oraz w sprawie swobodnego przepływu takich danych i uchylająca decyzję ramową Rady 2008/977/WSiSW zaczęła obowiązywać w maju 2018 r. Przedmiotowa dyrektywa stoi na straży podstawowego prawa obywateli do ochrony danych, gdy dane osobowe są wykorzystywane przez organy ścigania. Zapewnia ona należytą ochronę danych osobowych ofiar, świadków i podejrzanych o przestępstwa, a także ułatwia współpracę transgraniczną w walce z przestępczością i terroryzmem. 25 lipca 2022 r. Komisja Europejska opublikowała spóźnione sprawozdanie w sprawie stosowania i funkcjonowania dyrektywy o ochronie danych w sprawach karnych. Następnie przeprowadzono badanie oceniające zlecone przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE), zawierające krytyczną ocenę wdrożenia dyrektywy o ochronie danych w sprawach karnych.

c. Dyrektywa w sprawie prywatności i łączności elektronicznej

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) została zmieniona dyrektywą 2009/136/WE z dnia 25 listopada 2009 r. Poruszono w niej delikatną kwestię zatrzymywania danych, która była wielokrotnie przedkładana Trybunałowi Sprawiedliwości UE i doprowadziła do wydania szeregu orzeczeń, takich jak orzeczenie w 2020 r., w których stwierdzono, że prawo UE wyklucza ogólne i niezróżnicowane zatrzymywanie danych o ruchu i lokalizacji.

Wniosek z 2017 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych

w łączności elektronicznej i uchylający dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej) był przedmiotem przedłużających się dyskusji. Eksperci Parlamentu wskazali, że Parlament powinien sprzeciwić się podejmowanym przez Radę próbom wykluczenia stosowania europejskich zasad ochrony danych.

W lutym 2025 r. Komisja wskazała w swoim programie prac na rok 2025, że wycofa wniosek dotyczący nowego rozporządzenia o prywatności i łączności elektronicznej (zastępującego obecną dyrektywę o prywatności i łączności elektronicznej). W lipcu Komisja zatwierdziła wycofanie wniosku, które następnie opublikowano w Dzienniku Urzędowym w dniu 6 października. Obecna dyrektywa o prywatności i łączności elektronicznej oraz jej krajowe przepisy transponujące pozostają w mocy.

d. Rozporządzenie w sprawie przetwarzania danych osobowych przez instytucje i organy unijne

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 weszło w życie 11 grudnia 2018 r.

e. Artykuły dotyczące ochrony danych w sektorowych aktach ustawodawczych

Poza głównymi aktami ustawodawczymi dotyczącymi ochrony danych, o których mowa powyżej, szczegółowe przepisy dotyczące ochrony danych są również określone w sektorowych aktach ustawodawczych, takich jak:

— artykuł 13 (dotyczący ochrony danych osobowych) dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania;

— artykuł 4 (w sprawie gromadzenia danych) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2025/12 z 19 grudnia 2024 r. w sprawie gromadzenia i przekazywania danych pasażera przekazywanych przed podróżą w celu usprawnienia i ułatwienia kontroli na granicach zewnętrznych oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/13 z 19 grudnia 2024 r. w sprawie gromadzenia i przekazywania danych pasażera przekazywanych przed podróżą w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania;

— rozdział VI (dotyczący gwarancji ochrony danych) rozporządzenia (UE) 2016/794 Parlamentu Europejskiego i Rady z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol);

— rozdział VIII (dotyczący ochrony danych) rozporządzenia Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażającego wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej (EPPO);

— rozdział II rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) zakazuje szeregu praktyk w zakresie sztucznej inteligencji wiążących się z określonym wykorzystaniem danych, natomiast w rozdziale III nałożono obowiązek przeprowadzania ocen skutków dla ochrony danych w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka.

4. Główne ustalenia UE dotyczące przekazywania danych w obszarze transatlantyckim

a. Komercyjne przekazywanie danych – decyzje stwierdzające odpowiedni stopień ochrony i ramy ochrony danych UE–USA

Zgodnie z art. 45 ogólnego rozporządzenia o ochronie danych Komisja jest uprawniona do określenia, czy dane państwo spoza UE zapewnia odpowiedni poziom ochrony danych, czy to na podstawie jego przepisów krajowych czy podjętych przezeń zobowiązań międzynarodowych.

Chociaż przekazywanie danych między UE a Stanami Zjednoczonymi gwałtownie się nasiliło, a Stany Zjednoczone dominują w prywatnej reklamie internetowej i w nadzorze internetowym, Parlament przyjął liczne rezolucje, w których wyraża obawy dotyczące transatlantyckich przepływów danych. W szczególności Parlament uznał, że decyzja dotycząca Tarczy Prywatności UE–USA nie zapewnia odpowiedniego poziomu ochrony wymaganego prawem UE, a TSUE wielokrotnie unieważniał decyzje Komisji stwierdzające odpowiedni stopień ochrony w odniesieniu do Stanów Zjednoczonych (zob. wyroki Trybunału z 2015 r. w sprawie zasady bezpiecznej przystani w sprawie Schrems oraz z 2020 r. w sprawie Tarczy Prywatności UE–USA w sprawie Schrems II).

Pomimo braku reformy systemu ochrony danych w USA Komisja zawarła kolejne porozumienie ze Stanami Zjednoczonymi i przedstawiła wniosek dotyczący kolejnych ram ochrony danych między UE a USA. Na wniosek komisji LIBE 11 maja 2023 r. Parlament przyjął rezolucję w sprawie adekwatności ochrony zapewnianej przez ramy ochrony danych między UE a USA, w której stwierdził, że ramy te nie zapewniają zasadniczej równorzędności poziomu ochrony danych, oraz wezwał Komisję do kontynuowania negocjacji z amerykańskimi partnerami, ale do powstrzymania się od przyjęcia stwierdzenia adekwatności do czasu pełnego wdrożenia wszystkich zaleceń zawartych w rezolucji Parlamentu i opinii Europejskiej Rady Ochrony Danych.

10 lipca 2023 r. Komisja przyjęła trzecie ramy ochrony danych UE–USA. W wyroku z 3 września 2025 r. Sąd (sprawa T-553/23 *Latombe przeciwko Komisji Europejskiej*) oddalił skargę o stwierdzenie nieważności decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do ram ochrony danych UE–USA, utrzymując tym samym jej ważność. W komunikacie prasowym Sąd potwierdził, że „w dniu wydania zaskarżonej decyzji Stany Zjednoczone Ameryki zapewniały odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej do organizacji w tym państwie".

b. Umowa parasolowa UE–USA

W ramach procedury zgody Parlament uczestniczył w przyjęciu porozumienia między Stanami Zjednoczonymi a UE w sprawie ochrony informacji osobowych dotyczących zapobiegania przestępstwom, ich wykrywania, prowadzenia postępowań

przygotowawczych w ich sprawie i ich ścigania, znanego również jako umowa parasolowa. Celem tej umowy jest zagwarantowanie wysokiego poziomu ochrony informacji osobowych, które przekazuje się w ramach współpracy transatlantyckiej na rzecz ochrony porządku publicznego, a mianowicie w walce z terroryzmem i przestępczością zorganizowaną.

c. Program śledzenia przez UE i USA środków finansowych należących do terrorystów (TFTP)

Unia Europejska podpisała dwustronną umowę z USA dotyczącą przetwarzania i przekazywania z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów programu śledzenia środków finansowych należących do terrorystów.

5. Organy nadzorcze ds. ochrony danych

Europejski Inspektor Ochrony Danych (EIOD) to niezależny organ nadzorczy zapewniający, aby instytucje oraz organy UE przestrzegały swych zobowiązań w dziedzinie ochrony danych. Podstawowymi obowiązkami EIOD są nadzór, konsultacja i współpraca. EIOD bada skargi i doradza w sprawie polityki i przepisów, które mają wpływ na prywatność. EIOD informuje również o zagrożeniach oraz o ochronie praw i wolności osób podczas przetwarzania ich danych osobowych.

Europejska Rada Ochrony Danych, wcześniej Grupa Robocza Art. 29, ma status organu UE posiadającego osobowość prawną oraz niezależny sekretariat (udostępniany przez EIOD). W skład Europejskiej Rady Ochrony Danych wchodzą krajowe organy nadzoru UE, Europejski Inspektor Ochrony Danych oraz Komisja. Europejska Rada Ochrony Danych ma szerokie uprawnienia do rozstrzygania sporów między krajowymi organami nadzoru oraz udziela porad i wytycznych dotyczących kluczowych pojęć zawartych w dyrektywie w sprawie ogólnego rozporządzenia o ochronie danych i dyrektywie w sprawie egzekwowania prawa.

ROLA PARLAMENTU EUROPEJSKIEGO

Parlament odegrał kluczową rolę w kształtowaniu prawodawstwa UE w dziedzinie ochrony danych osobowych, nadając ochronie prywatności priorytet polityczny. Ponadto w ramach zwykłej procedury ustawodawczej prowadził – na równi z Radą – prace nad reformą ochrony danych.

W wielu rezolucjach Parlament wyrażał wątpliwości co do adekwatności ochrony przyznanej obywatelom UE w ramach programu UE i USA „Bezpieczna przystań", a następnie porozumienia o Tarczy Prywatności UE–USA. Po tym, jak sprawa Schrems II doprowadziła do unieważnienia decyzji wykonawczej Komisji (UE) 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA, a to w związku z obawami, że uprawnienia rządu USA w zakresie nadzoru nie były ograniczone, czego wymaga prawo UE, oraz że obywatele UE nie mieli skutecznych środków odwoławczych, Parlament przyjął rezolucję, w której wyraził ubolewanie, że stosunki ze Stanami Zjednoczonymi były dla Komisji ważniejsze od interesów obywateli UE.

Po przedłożeniu projektu przez komisję LIBE Parlament w dniu 11 maja 2023 r. przyjął rezolucję w sprawie adekwatności ochrony zapewnianej przez ramy ochrony

danych między UE a USA, w której stwierdził, że ramy te nie zapewniają zasadniczej równorzędności poziomu ochrony danych, oraz wezwał Komisję do kontynuowania negocjacji z amerykańskimi partnerami, ale do powstrzymania się od przyjęcia stwierdzenia adekwatności do czasu pełnego wdrożenia wszystkich zaleceń zawartych w rezolucji i opinii EROD. 10 lipca 2023 r. Komisja przyjęła decyzję w sprawie ram ochrony danych UE–USA.

Parlament wielokrotnie potępiał amerykańskie praktyki inwigilacyjne. We wrześniu 2001 r. przyjął rezolucję w sprawie istnienia globalnego systemu ECHELON do przechwytywania wiadomości prywatnych i handlowych. Po doniesieniach Edwarda Snowdena w marcu 2014 r. Parlament przyjął rezolucję w sprawie realizowanego przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA) programu nadzoru i organów nadzoru w różnych państwach członkowskich, a następnie w październiku 2015 r. przyjął rezolucję w tej sprawie.

Parlament powołał komisję śledczą ds. zbadania stosowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego do inwigilacji w państwach członkowskich UE (PEGA). Pod przewodnictwem posła do PE Jeroena Lenaersa komisja PEGA szczegółowo zbadała wykorzystywanie oprogramowania szpiegowskiego do prowadzenia dochodzeń w sprawie członków opozycji, dziennikarzy, prawników i działaczy społeczeństwa obywatelskiego, a także wpływ takich praktyk na procesy demokratyczne i indywidualne prawa w UE. W trakcie dochodzenia komisja PEGA zasięgnęła opinii czołowych naukowców, praktyków i władz w UE i na całym świecie. Departament tematyczny Parlamentu przygotował sprawozdania z misji PEGA w Polsce, w Grecji i na Cyprze. 8 maja 2023 r. komisja PEGA głosowała nad zatwierdzeniem sprawozdania końcowego (sprawozdawczyni: Sophia in ‘t Veld) dotyczącego dochodzenia w sprawie domniemanych naruszeń i niewłaściwego administrowania w stosowaniu prawa UE w odniesieniu do wykorzystywania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji, a także m.in. zalecenia utworzenia unijnego laboratorium technologicznego do celów badań i monitorowania stosowania oprogramowania szpiegowskiego przeciwko obywatelom UE. Zalecenie Parlamentu dla Rady i Komisji w następstwie sprawozdania komisji PEGA zostało przyjęte na posiedzeniu plenarnym 15 czerwca 2023 r. Komisja nie odpowiedziała jednak w odpowiednim czasie na zalecenie i zablokowała projekt pilotażowy unijnego laboratorium technologicznego zaproponowany przez posłów do Parlamentu Europejskiego. W listopadzie 2023 r. Parlament przyjął rezolucję w sprawie niepodjęcia działań legislacyjnych przez Komisję w związku z rezolucją w sprawie komisji PEGA, a w czerwcu 2025 r. przeprowadził również debatę na temat aktualnej sytuacji i działań następczych dwa lata po zaleceniach komisji PEGA oraz na temat nielegalnego stosowania oprogramowania szpiegowskiego.

13 marca 2024 r. Parlament przyjął rezolucję ustawodawczą w sprawie wniosku dotyczącego rozporządzenia ustanawiającego zharmonizowane przepisy z zakresu sztucznej inteligencji (akt w sprawie sztucznej inteligencji). W przyjętym 13 czerwca 2024 r. rozporządzeniu (UE) 2024/1689 ustanowiono obowiązki spoczywające na systemach i dostawcach sztucznej inteligencji w oparciu o potencjalne ryzyko i skutki związane ze sztuczną inteligencją. Systemy sztucznej inteligencji uznane za wyraźne zagrożenie dla praw podstawowych jednostki (w tym dla ochrony danych) będą

zakazane. Akt w sprawie sztucznej inteligencji wszedł w życie 1 sierpnia 2024 r. Większość przepisów tego aktu zacznie obowiązywać 2 sierpnia 2026 r.

Parlament zlecił szereg badań naukowych w celu uzyskania podstawy naukowej dla swoich działań ustawodawczych podejmowanych z myślą o rozwoju sytuacji w zakresie technologii i ochrony danych, w tym badanie dotyczące wpływu ogólnego rozporządzenia o ochronie danych na sztuczną inteligencję, badanie dotyczące biometrii i detekcji zachowań, badanie dotyczące danych pasażera przekazywanych przed podróżą – analiza wniosków Komisji Europejskiej w sprawie zreformowania ram prawnych dotyczących danych pasażera przekazywanych przed podróżą, a także badanie na temat prawa oraz technologii informacyjnych i komunikacyjnych.

Parlament przeanalizuje przyszłe inicjatywy polityczne i wnioski ustawodawcze dotyczące zatrzymywania danych, szyfrowania i uprawnionego przechwytywania danych, które to inicjatywy i wnioski zapowiedziano w planie działania Komisji na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych, opublikowanym 24 czerwca 2025 r., oraz przeprowadzi głosowanie w ich sprawie.

Mariusz Maciejewski / Alessandro Davoli
04/2026