OCHRONA DANYCH OSOBOWYCH

Ochrona danych osobowych i poszanowanie życia prywatnego to ważne prawa podstawowe. 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 zwiększające 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 UE.

CELE

Unia musi dopilnować, by podstawowe prawo do ochrony danych, przewidziane w Karcie praw podstawowych UE, było konsekwentnie przestrzegane. Należy wzmocnić stanowisko UE w sprawie ochrony danych osobowych w kontekście wszystkich strategii politycznych UE, w tym egzekwowania prawa i zapobiegania przestępczości, a także w stosunkach międzynarodowych, zwłaszcza w społeczeństwie globalnym charakteryzującym się szybkimi zmianami technologicznymi.

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) a 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. Art. 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 UE 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 (EKPC)

W art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r. zapisano prawo do poszanowania życia prywatnego i rodzinnego: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej 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 wyraźną zgodę 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 będzie można zastosować środki naprawcze, takie jak ostrzeżenia i nakazy lub kary finansowe.

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.

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.

Obecnie rozpatrywany jest nowy wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej).

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 w dniu 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;

— 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”).

4. Główne ustalenia międzynarodowe UE dotyczące przekazywania danych

a. Komercyjne przekazywanie danych: decyzje stwierdzające odpowiedni stopień ochrony

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 zobowiązań międzynarodowych.

Parlament przyjął szereg rezolucji, w których wyraził obawy dotyczące transatlantyckich przepływów danych.

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. Umowy między UE a USA, UE a Australią oraz między UE a Kanadą dotyczące danych PNR

UE podpisała dwustronne umowy w sprawie danych dotyczących przelotu pasażera (PNR) ze Stanami Zjednoczonymi, Australią i Kanadą. Dane PNR obejmują informacje dostarczane przez pasażerów podczas dokonywania rezerwacji lub odprawy przed lotem oraz dane gromadzone przez przewoźników lotniczych do własnych celów handlowych. Dane PNR mogą być wykorzystywane przez organy ścigania do zwalczania poważnej przestępczości i terroryzmu.

d. 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. Uwzględnienie aspektów ochrony danych w rezolucjach sektorowych

Szereg rezolucji Parlamentu na temat różnych obszarów polityki dotyczy również ochrony danych osobowych w celu zapewnienia spójności z ogólnymi przepisami UE dotyczącymi ochrony danych oraz ochrony prywatności w tych konkretnych sektorach.

6. 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.

Europejska Rada Ochrony Danych, wcześniej Grupa Robocza Art. 29, ma status organu UE posiadającego osobowość prawną oraz niezależny sekretariat. 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. Zakończył również prace nad ostatnim istotnym aktem prawnym w tym obszarze – nowym rozporządzeniem o prywatności i łączności elektronicznej i ze zniecierpliwieniem oczekuje, że Rada ostatecznie zakończy swoje prace w celu rozpoczęcia negocjacji.

Parlament ściśle nadzorował międzynarodowe porozumienia dotyczące przekazywania danych. Za pomocą procedury zgody lub sprawozdań z własnej inicjatywy dopilnował, aby jego głos został usłyszany. Ponadto przed głosowaniem nad umową w sprawie PNR między UE a Kanadą Parlament postanowił zwrócić się w formie rezolucji z dnia 25 listopada 2014 r. do Trybunału Sprawiedliwości o wydanie opinii, o której mowa w art. 218 ust. 1 TFUE. W opinii wydanej w dniu 26 lipca 2017 r. Trybunał stwierdził, że umowa w sprawie PNR nie mogła zostać zawarta w jej ówczesnej formie, ponieważ niektóre postanowienia były niezgodne z podstawowym prawem do ochrony danych osobowych.

Zapewniwszy właściwe wprowadzenie unijnych przepisów dotyczących ochrony danych, Parlament najprawdopodobniej skupi się obecnie na monitorowaniu wdrażania prawodawstwa.

Kristiina Milt
05/2019