Oświadczenie nr 02/2021 w sprawie nowego projektu przepisów drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (konwencja budapeszteńska)

Przyjęte 2 lutego 2021 r.

Europejska Rada Ochrony Danych (EROD) przyjęła następujące oświadczenie:

Uwagi wstępne oraz kontekst oświadczenia EROD

Europejska Rada Ochrony Danych (EROD) oraz unijne organy ochrony danych z uwagą obserwują rozwój prac nad drugim protokołem dodatkowym do konwencji budapeszteńskiej i regularnie uczestniczą w konsultacjach prowadzonych przez Radę Europy, takich jak doroczna „konferencja Octopus". W listopadzie 2019 r. EROD opublikowała również swój najnowszy wkład do konsultacji nad projektem drugiego protokołu dodatkowego[1], zaznaczając, iż pozostaje ona „otwarta na dodatkowe wkłady" oraz zaapelowała o „wczesne oraz bardziej aktywne zaangażowanie organów ochrony danych w przygotowanie przepisów szczegółowych protokołu w celu zapewnienia optymalnego zrozumienia oraz uwzględnienia zabezpieczeń w zakresie ochrony danych"[2].

W związku z opublikowaniem nowego projektu przepisów drugiego protokołu dodatkowego do konwencji budapeszteńskiej[3] EROD pragnie ponownie zapewnić ekspercki, konstruktywny wkład, mając na celu należyte uwzględnienie kwestii ochrony danych osobowych w procesie opracowywania protokołu dodatkowego, biorąc pod uwagę, że spotkania poświęcone przygotowaniu protokołu dodatkowego odbywają się na zamkniętych posiedzeniach oraz że w warunkach przygotowania

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf
[2] EROD podtrzymuje stanowiska i zalecenia wyrażone w swoim poprzednim wkładzie oraz uważa za istotne przypomnienie kluczowych zasad w świetle aktualnego stanu prac nad protokołem oraz opublikowanego nowego projektu przepisów.
[3] https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations

opracowanych przez T-CY[4] nie przewidziano bezpośredniego zaangażowania organów ochrony danych w proces przygotowawczy.

Ponadto EROD uważa, że wspomniane wyżej przepisy mogą mieć wpływ na materialne i formalne warunki dostępu do danych osobowych w UE, w tym dostępu udzielanego na wniosek organów państw trzecich, co jest zbieżne z toczącymi się dyskusjami na szczeblu UE oraz powiązanymi inicjatywami ustawodawczymi analizowanymi obecnie przez współprawodawców[5]. EROD apeluje zatem do Komisji Europejskiej oraz Parlamentu Europejskiego, jak również do państw członkowskich UE i parlamentów narodowych, aby uważnie monitorowały toczące się negocjacje w celu zagwarantowania całkowitej zgodności planowanego drugiego protokołu dodatkowego z dorobkiem prawnym UE, zwłaszcza w zakresie ochrony danych osobowych.

Kwestia dostępu do danych osobowych pomiędzy jurysdykcjami była już w przeszłości poruszana przez organy ochrony danych UE w różnych stanowiskach i opiniach na ten temat, ale EROD pragnie ponownie przywołać uwagi Grupy Roboczej Art. 29 dotyczące bezpośredniego dostępu organów ścigania państw trzecich do danych przechowywanych przez inne państwa, przedstawione w projekcie fragmentów protokołu dodatkowego do konwencji budapeszteńskiej o cyberprzestępczości[6], jak również oświadczenie tej Grupy w sprawie aspektów ochrony danych i prywatności związanych z transgranicznym dostępem do elektronicznego materiału dowodowego[7]. Europejski Inspektor Ochrony Danych (EIOD) wydał opinię 03/2019 w sprawie mandatu do udziału Komisji w negocjacjach[8], jak również opinię 7/2019 w sprawie wniosków dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów dotyczących elektronicznego materiału dowodowego w sprawach karnych[9]. Wkład ten opiera się również na opinii 23/2018 wydanej przez EROD w sprawie wniosków Komisji dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów dotyczących elektronicznego materiału dowodowego w sprawach karnych[10].

EROD jest w pełni świadoma, że jeżeli organy wymiaru sprawiedliwości i organy ścigania mają do czynienia w swoich dochodzeniach z „sytuacją transgraniczną" w kwestii dostępu do danych osobowych, może to stanowić wyzwanie, a także dostrzega zasadność dążenia do poprawy

[4] Warunki przygotowania projektu drugiego protokołu dodatkowego do konwencji budapeszteńskiej o cyberprzestępczości, przyjęte na 17. posiedzeniu plenarnym komisji ds. Konwencji o cyberprzestępczości dnia 8 czerwca 2017 r., T-CY (2017)3.

[5] W szczególności dotyczy to dyskusji w sprawie wniosków Komisji dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów dotyczących elektronicznego materiału dowodowego w sprawach karnych.

[6] Uwagi Grupy Roboczej Art. 29 dotyczące kwestii bezpośredniego dostępu organów ścigania państw trzecich do danych przechowywanych w ramach jurysdykcji innego państwa, zaproponowane w projekcie fragmentów protokołu dodatkowego do konwencji budapeszteńskiej o cyberprzestępczości, 5.12.2013 r.

[7] Oświadczenie Grupy Roboczej Art. 29 w sprawie aspektów ochrony danych i prywatności związanych z transgranicznym dostępem do elektronicznego materiału dowodowego, 29 listopada 2017 r.

[8] Opinia EIOD 3/2019 dotycząca uczestnictwa w negocjacjach dotyczących drugiego protokołu dodatkowego do budapeszteńskiej konwencji o cyberprzestępczości.

[9] Opinia EIOD 7/2019 w sprawie wniosków dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów dotyczących elektronicznego materiału dowodowego w sprawach karnych.

[10] Opinia EROD 23/2018 przyjęta dnia 26 września 2018 r. w sprawie wniosków Komisji dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów dotyczących elektronicznego materiału dowodowego w sprawach karnych.

międzynarodowej współpracy w zakresie cyberprzestępczości oraz dostępu do informacji. Jednocześnie EROD przypomina, że należy zagwarantować ochronę danych osobowych oraz pewność prawną, przyczyniając się tym samym do zapewnienia zrównoważonych warunków wymiany danych osobowych z państwami trzecimi do celów egzekwowania prawa, które to warunki byłyby także w pełni zgodne z Traktatami UE i Kartą praw podstawowych. Ponadto EROD uważa za niezbędne, aby prace nad protokołem dodatkowym odbywały się z poszanowaniem podstawowych wartości i zasad Rady Europy, a zwłaszcza praw człowieka oraz praworządności.

W odniesieniu do „transgranicznego dostępu bezpośredniego do przechowywanych danych informatycznych", zgodnie z art. 32 lit. b konwencji budapeszteńskiej, EROD podkreśla w szczególności, że administrator danych może co do zasady ujawniać dane tylko po uprzednim przedstawieniu przez państwowy organ ścigania – zgodnie z jego prawem krajowym i ze wskazaniem, do jakiego celu dane te są wymagane – zezwolenia lub nakazu sądowego, lub jakiegokolwiek dokumentu uzasadniającego konieczność uzyskania dostępu do danych i odnoszącego się do odpowiedniej podstawy prawnej zezwalającej na ten dostęp.

Jako że konwencja budapeszteńska, jak również wszystkie zawarte w niej protokoły dodatkowe stanowią wiążące instrumenty międzynarodowe, EROD podkreśla, że zgodnie z orzecznictwem TSUE „zobowiązania nałożone umową międzynarodową nie mogą skutkować naruszeniem zasad konstytucyjnych traktatu WE, wśród których znajduje się zasada, zgodnie z którą wszystkie akty wspólnotowe powinny przestrzegać praw podstawowych, przy czym przestrzeganie to stanowi przesłankę ich zgodności z prawem"[11]. Konieczne jest zatem, aby podmioty negocjujące w imieniu UE zapewniły zgodność przepisów zawartych w protokole dodatkowym z dorobkiem unijnym w zakresie ochrony danych w celu zapewnienia spójności protokołu z unijnym prawem pierwotnym i wtórnym.

Biorąc pod uwagę ramy czasowe procesu konsultacji, wkład EROD będzie dotyczył wstępnej oceny nowego projektu przepisów drugiego protokołu konwencji budapeszteńskiej, który nie został wcześniej poddany konsultacjom z zainteresowanymi stronami:

- wspólne zespoły śledcze i wspólne śledztwa,
- niezwłoczne ujawnienie przechowywanych danych informatycznych w sytuacji nadzwyczajnej,
- wniosek o informacje na temat rejestracji nazw domen.

Jak już wspomniano, EROD ma świadomość, że specjalne przepisy dotyczące ochrony danych osobowych są w dalszym ciągu w trakcie omawiania. EROD pozostaje do dyspozycji w kwestii dalszych wkładów i apeluje o wczesne oraz aktywniejsze zaangażowanie organów ochrony danych w przygotowanie wspomnianych przepisów szczegółowych w celu zapewnienia optymalnego zrozumienia oraz uwzględnienia zabezpieczeń w zakresie ochrony danych.

[11] Zob. TSUE sprawy połączone C-402/05 P i C-415/05 P, Kadi / Rada, ECLI:EU:C:2008:461, pkt 285.

Wstępny projekt przepisów dotyczących wspólnych zespołów śledczych i wspólnych śledztw (JITs) (art. 3), wniosku o informacje na temat rejestracji nazw domen (art. 6) oraz niezwłocznego ujawniania przechowywanych danych informatycznych w sytuacji nadzwyczajnej (art. 7)

Na podstawie przeprowadzonej oceny wstępnej EROD zaleca dalszą analizę wstępnego projektu przepisów w odniesieniu do następujących elementów.

EROD zauważa, że zarówno wnioski o informacje na temat rejestracji nazw domen, jak i o niezwłoczne ujawnianie przechowywanych danych informatycznych w sytuacjach nadzwyczajnych nie są wnioskami wiążącymi, a podstawy do odmowy zrealizowania wniosku nie są ściśle określone, podczas gdy możliwość powołania się na prawo wezwanego państwa strony w celu odmowy takiej współpracy, w tym podstawy odmowy określone w traktatach o pomocy prawnej, są również niejasne[12]. W odniesieniu do tego EROD przypomina, że warunki, na jakich dostawcy usług łączności elektronicznej lub podmiot dostarczający usługi nazw domen mają udzielać owego dostępu, muszą być przewidziane ustawą, aby zapewnić oparcie przetwarzania danych na jasnych podstawach prawnych.

Dodatkowo, EROD odnosi się do swojego wcześniejszego wkładu, aby ponownie poinformować, że oprócz przypadków należycie stwierdzonej pilnej potrzeby,[13] oraz, w świetle orzecznictwa TSUE[14], EROD uważa, że organy mogące składać tego rodzaju wniosek powinny ograniczać się do: prokuratora, organu wymiaru sprawiedliwości lub innego niezależnego organu. EROD uważa również, że systematyczne angażowanie organów wymiaru sprawiedliwości jako stron wezwanych jest niezbędne do zapewnienia skutecznej kontroli zgodności wniosków z konwencją oraz do dalszego stosowania zasady podwójnej karalności czynu w dziedzinie współpracy sądowej.

W tej kwestii EROD przypomina jednak, że zasada podwójnej karalności czynu służy dodatkowemu zabezpieczeniu tego, aby jedna ze stron nie mogła zdać się na pomoc innej strony w zastosowaniu sankcji karnej, która nie jest przewidziana w prawie tej drugiej strony. Oprócz zapewnienia poszanowania praw osób fizycznych oraz sprawiedliwości proceduralnej w ramach planowanego mechanizmu współpracy sądowej, takie zabezpieczenie dostarcza również istotnej gwarancji przestrzegania warunków formalnych obowiązujących przy dostępie do danych osobowych tych osób. Jak zostało już wspomniane w ramach poprzedniego wkładu dotyczącego kwestii bezpieczeństwa przetwarzania danych, EROD zwraca się do T-CY o rozważenie, jako szczególnego zabezpieczenia w zakresie ochrony danych, zastosowania mechanizmu bezzwłocznego powiadamiania o naruszeniach ochrony danych, które mogą w poważnym stopniu ingerować w prawa oraz wolności osób fizycznych, których te dane dotyczą. Naruszenia danych osobowych mogą bowiem wywoływać szereg istotnych, negatywnych skutków dla osób fizycznych, których te dane dotyczą.

W odniesieniu do wstępnego projektu przepisów dotyczących wniosku o informacje na temat rejestracji nazw domen EROD podkreśla, że informacje te zawierają dane osobowe i w związku z tym wszelkie instrumenty międzynarodowe określające materialne oraz formalne warunki dostępu do

[12] Projekt art. 6 ust. 2 odnosi się na przykład do „rozsądnych warunków przewidzianych w prawie krajowym".

[13] EROD zauważa, że pojęcie sytuacji nadzwyczajnej występuje tu w rozumieniu ust. 1 projektu przepisu dotyczącego wzajemnej pomocy w sytuacjach nadzwyczajnych, oraz uważa, że zakres przedmiotowy takiej sytuacji mógłby zostać dookreślony i dopracowany.

[14] Zob. TSUE sprawy połączone C-203/15 i C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, pkt 120.

takich danych muszą być zgodne, w przypadku stron będących członkami Unii Europejskiej, z unijnym prawem pierwotnym i wtórnym.

W kwestii wstępnego projektu przepisów dotyczących „niezwłocznego ujawnienia przechowywanych danych informatycznych w sytuacji nadzwyczajnej" (art. 7) EROD zauważa, że w zależności od sposobu zastosowania tego przepisu przez każdą ze stron może się on wiązać z bezpośrednim ujawnianiem danych dotyczących treści. EROD zauważa również, że wezwane państwo-strona może wymagać, po ujawnieniu danych, zapewnienia właściwego wniosku o wzajemną pomoc (art. 7 ust. 5). W przypadku tej drugiej kwestii strony planowanego protokołu nie są jednak zobowiązane do usuwania danych czy do nieużywania ich jako dowodów, jeśli na podstawie informacji uzupełniających uzyskanych we właściwym wniosku o wzajemną pomoc wezwane organy stwierdzą, że warunki niezbędne do ujawnienia danych nie zostały spełnione. W rezultacie wydaje się, że skutki prawne ujawnienia danych, gdy są one już dostępne dla państwa wnioskującego, pozostają całkowicie w gestii prawa krajowego danego państwa. Zatem brak zawarcia w protokole elementu zobowiązującego wiąże się z ryzykiem pozbawienia tego przepisu jakiegokolwiek skutku ochronnego w odniesieniu do przetwarzania już ujawnionych danych osobowych.

EROD podkreśla ponadto wymóg wynikający z art. 52 ust. 1 Karty praw podstawowych UE[15], zgodnie z którym wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie podlegają zasadzie proporcjonalności i mogą być wprowadzone wyłącznie wtedy, gdy są niezbędne. Zatem projekt przepisów planowanego protokołu musi spełniać ten wymóg, aby być zgodnym z prawem UE. Wymóg ten dotyczy zarówno danych osobowych zawartych we wniosku, jak i w odpowiedzi na taki wniosek. **EROD jest zatem szczególnie zaniepokojona brzmieniem projektu art. 6 ust. 3 lit. c) oraz, odnoszącego się do tego przepisu, pkt 13. projektu sprawozdania wyjaśniającego, które wydają się sugerować, że wnioskujące państwa trzecie będące stronami planowanego protokołu mogą nie być zobowiązane do przestrzegania zasady proporcjonalności przy składaniu wniosków do państwa członkowskiego UE.** Ponadto nie ma pełnej jasności co do możliwości powoływania się na zasadę proporcjonalności jako podstawę odmowy na podstawie tych przepisów.

Nie jest również jasne, czy strony byłyby związane zobowiązaniami do zapewnienia, w kontekście planowanego protokołu, warunków i zabezpieczeń określonych w art. 15 konwencji budapeszteńskiej[16]. **EROD zaleca wyjaśnienie, czy zobowiązania określone w art. 15 konwencji budapeszteńskiej mają pełne zastosowanie również w kontekście omawianej współpracy transgranicznej.**

<u>Przepisy dotyczące zabezpieczeń w zakresie ochrony danych</u>

EROD uważa za niezbędne, aby upubliczniony tekst wstępny był uzupełniony o specjalne przepisy dotyczące zabezpieczeń w zakresie ochrony danych, które następnie należy ocenić wraz z innymi przepisami, aby zapewnić przełożenie się projektu protokołu dodatkowego na zrównoważoną wymianę danych osobowych z państwami trzecimi do celów egzekwowania prawa, która jest w pełni zgodna z Traktatami UE i Kartą praw podstawowych.

[15] Zob. też art. 8 ust. 2 europejskiej konwencji praw człowieka.
[16] Zob. w szczególności art. 6 ust. 4 w nawiasach.

Wstępny projekt przepisów dotyczących: wniosku o informacje na temat rejestracji nazw domen oraz niezwłocznego ujawnienia przechowywanych danych informatycznych w sytuacji nadzwyczajnej na skutek ustanowienia warunków formalnych dostępu do danych osobowych może już wpływać na stopień ochrony danych osobowych oraz może również wymagać zmiany w celu zapewnienia praktycznego zastosowania odpowiednich zabezpieczeń w zakresie ochrony danych. **W odniesieniu do tego EROD pragnie ponownie podkreślić konieczność zastosowania zabezpieczeń w zakresie ochrony danych do wszelkiej wymiany danych osobowych w kontekście planowanego protokołu[17], w tym w odniesieniu do przekazywania danych osobowych[18].**

EROD uważa, że przepisy szczegółowe dotyczące zabezpieczeń w zakresie ochrony danych muszą odzwierciedlać kluczowe zasady, a zwłaszcza: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizację danych, prawidłowość, ograniczenie przechowywania, integralność i poufność. EROD pragnie również podkreślić znaczenie zapewnienia podstawowych praw indywidualnych (prawa do: dostępu, sprostowania, usunięcia), przy jednoczesnym ograniczeniu wszelkich restrykcji zasadą proporcjonalności, oraz znaczenie skutecznych środków zaskarżenia dostępnych dla osób, których dane dotyczą, w przypadku naruszenia zabezpieczeń w zakresie ochrony danych. Przy wykonywaniu tych praw konieczne jest również powiadomienie osoby, której dane dotyczą, w sytuacji gdy nie stanowi to już zagrożenia dla przebiegu dochodzenia. Wspomniane zasady, prawa i obowiązki są również zgodne ze zaktualizowaną Konwencją Rady Europy o ochronie osób w związku z przetwarzaniem danych osobowych (Konwencja 108+), do której przystąpiło również wiele stron konwencji budapeszteńskiej o cyberprzestępczości. Zgodnie z Konwencją 108+ zasady, prawa i obowiązki powinny mieć zastosowanie do wszystkich organów przetwarzających dane w ramach strony wnioskującej w celu zapewnienia ciągłości ochrony. **Szczegółowe informacje dotyczące wymogów UE w tym zakresie znajdują się we wkładzie EROD przygotowanym na potrzeby konsultacji publicznych przeprowadzonych w 2019 r.**[19]

EROD ponownie podkreśla znaczenie zaangażowania organów ochrony danych w proces opracowania protokołu dodatkowego i wyraża swoją gotowość do wniesienia wkładu i wsparcia T-CY w przygotowaniu wstępnego tekstu przepisów dotyczących zabezpieczeń w zakresie ochrony danych.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[17] Art. 6 ust. 4 wydaje się ograniczać stosowanie zabezpieczeń, jak również stosowanie art. 15 konwencji tylko do przypadków ujawniania informacji, z pominięciem przypadków ujawniania danych osobowych zawartych we wniosku.

[18] Zgodnie z pkt 9 projektu sprawozdania wyjaśniającego drugi z tych przepisów może/powinien mieć zastosowanie tylko w przypadku przekazywania danych osobowych do wspólnych zespołów śledczych.

[19] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf