Oświadczenie 03/2021 w sprawie rozporządzenia w sprawie prywatności i łączności elektronicznej

przyjęte 9 marca 2021 r.

Europejska Rada Ochrony Danych (EROD) przyjęła następujące oświadczenie:

EROD z zadowoleniem przyjmuje uzgodniony mandat negocjacyjny przyjęty przez Radę w sprawie zmiany przepisów o ochronie prywatności i poufności w usługach łączności elektronicznej („stanowisko Rady") jako pozytywny krok w kierunku nowego rozporządzenia w sprawie prywatności i łączności elektronicznej. Niezwykle ważne jest, aby ogólne ramy ochrony danych UE zostały szybko uzupełnione zharmonizowanymi przepisami dotyczącymi łączności elektronicznej.

Jak to już wielokrotnie stwierdzano[1], rozporządzenie w sprawie prywatności i łączności elektronicznej w żadnym przypadku nie może obniżać stopnia ochrony zapewnianego przez obowiązującą dyrektywę o prywatności i łączności elektronicznej, lecz powinno uzupełniać ogólne rozporządzenie o ochronie danych (RODO) zapewniając dodatkowe silne gwarancje w zakresie poufności i ochrony wszystkich rodzajów łączności elektronicznej. Rozporządzenie w sprawie prywatności i łączności elektronicznej w żadnym przypadku nie może być wykorzystywane do faktycznej zmiany RODO. W tym względzie stanowisko Rady budzi szereg obaw, a EROD pragnie zwrócić uwagę na kwestie, które należy uwzględnić w nadchodzących negocjacjach.

Oświadczenie to pozostaje bez uszczerbku dla ewentualnego przyszłego bardziej szczegółowego oświadczenia lub opinii EROD na temat stanowisk współprawodawców.

Obawy dotyczące przetwarzania i zatrzymywania danych pochodzących z łączności elektronicznej do celów egzekwowania prawa i ochrony bezpieczeństwa narodowego

W odniesieniu do art. 6 ust. 1 lit. d) i art. 7 ust. 4 EROD potwierdza, że środki ustawodawcze wymagające od dostawców usług łączności elektronicznej zatrzymywania danych pochodzących z łączności elektronicznej muszą być zgodne z:

- art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karta"),
- najnowszym orzecznictwem Trybunału Sprawiedliwości UE („TSUE")[2] oraz
- art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

[1] Zob. pełny wykaz dokumentów dotyczących zasad prywatności i łączności elektronicznej opracowanych przez EROD i Grupę Roboczą Art. 29 w załączniku do niniejszego oświadczenia.
[2] TSUE, sprawy połączone C-511/18, C-512/18 i C-520/18 oraz sprawa C-623/17.

EROD uważa, że rozporządzenie w sprawie prywatności i łączności elektronicznej nie może stanowić odstępstwa od stosowania najnowszego orzecznictwa TSUE, które stanowi w szczególności, że art. 7, 8, 11 i art. 52 ust. 1 Karty należy interpretować w ten sposób, że stoi on na przeszkodzie środkom ustawodawczym przewidującym prewencyjne uogólnienie i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji. W związku z tym, zapewnianie podstawy prawnej dla czegokolwiek innego niż ukierunkowanego zatrzymywania danych do celów egzekwowania prawa i ochrony bezpieczeństwa narodowego nie jest dozwolone na mocy Karty i w każdym przypadku musiałoby podlegać ścisłym ograniczeniom czasowym i materialnym, a także kontroli ze strony Trybunału lub niezależnego organu.

Jeżeli chodzi o wyłączenie z zakresu stosowania rozporządzenia czynności przetwarzania dokonywanych przez dostawców, EROD uważa, że takie wyłączenie jest sprzeczne z założeniem spójnych unijnych ram ochrony danych. EROD podkreśla jednak, że w przypadku wykluczenia zastosowanie ma RODO.

Poufność łączności elektronicznej wymaga szczególnej ochrony (art. 6, 6a, 6b, 6c)

Poufność komunikacji jest prawem podstawowym chronionym na mocy art. 7 Karty, wdrożonym już na mocy dyrektywy o prywatności i łączności elektronicznej. Prawo do zachowania poufności musi być stosowane do każdego rodzaju łączności elektronicznej, niezależnie od środków wykorzystywanych do przesłania , czy to w trakcie przesyłu, czy w oczekiwaniu na przesył, na każdym etapie od wysłania do doręczenia (od nadawcy do odbiorcy). Ochrony wymaga również integralność urządzeń końcowych każdego użytkownika.

Ogólne zakazy z wąskimi wyjątkami dotyczące przetwarzania danych osobowych

EROD w pełni popiera podejście oparte na ogólnych zakazach z wąskimi, konkretnymi i jasno zdefiniowanymi (ukierunkowanymi na cel) wyjątkami.

EROD obawia się jednak, że niektóre wprowadzone przez Radę wyjątki (w szczególności art. 6 ust. 1 lit. c), art. 6b ust. 1 lit. e), art. 6b ust. 1 lit. f), art. 6c) wydają się dopuszczać bardzo szerokie rodzaje przetwarzania, i przypomina o potrzebie zawężenia tych wyjątków do konkretnych i jasno określonych celów. W każdym przypadku te konkretne cele powinny być wyraźnie wymienione w celu zapewnienia pewności prawa i możliwie najwyższego stopnia ochrony.

Ponadto wyjątki przewidziane w art. 6 ust. 1 lit. b), c) i d), umożliwiające dostęp do danych pochodzących z łączności elektronicznej, łącznie z treścią, w celu zapewnienia bezpieczeństwa sieci i sprzętu użytkownika końcowego mogłyby umożliwić dostawcy usług łączności elektronicznej lub jego podmiotom przetwarzającym pełny dostęp do treści wszystkich komunikatów użytkownika końcowego. Ponieważ mogłoby to zagrozić prawu użytkownika końcowego do poufności i prywatności, należy zachować proporcjonalność i powinno być zawężone przynajmniej, aby przypomnieć, że nie może to prowadzić do systematycznego monitorowania treści łączności elektronicznej ani umożliwiać dostawcom usług i podmiotom przetwarzającym omijania jakiegokolwiek szyfrowania.

Ponadto w rozporządzeniu należy podkreślić rolę anonimizacji jako podstawowej gwarancji, która powinna być systematycznie preferowana przy wykorzystywaniu danych pochodzących z łączności elektronicznej.

Dostępność silnego i wiarygodnego szyfrowania jest niezbędna w nowoczesnym świecie cyfrowym.

Silne najnowocześniejsze szyfrowanie powinno być ogólną zasadą zapewniającą bezpieczny, swobodny i niezawodny przepływ danych między obywatelami, przedsiębiorstwami i władzami. Ma ono także kluczowe znaczenie dla zapewnienia bezpieczeństwa zgodnie z wymogami RODO, na przykład w odniesieniu do danych dotyczących zdrowia oraz dla ochrony systemów informatycznych w kontekście rosnących zagrożeń. Pełne szyfrowanie transmisji, od nadawcy do odbiorcy, jest również jedynym sposobem zapewnienia pełnej ochrony przekazywanych danych. Wszelkie ewentualne próby osłabienia szyfrowania, nawet w celach takich jak bezpieczeństwo narodowe, całkowicie pozbawiłyby skuteczności te mechanizmy ochrony ze względu na ich ewentualne bezprawne wykorzystanie. Szyfrowanie musi pozostać standaryzowane, silne i skuteczne[3].

Nowe rozporządzenie musi egzekwować wymóg uzyskania zgody na pliki cookie i podobne technologie oraz musi oferować dostawcom usług narzędzia techniczne umożliwiające im łatwe uzyskanie takiej zgody (art. 8[4]).

Potrzeba podejścia zapewniającego zachowanie prywatności w odniesieniu do rozwiązań „zaakceptuj lub odrzuć"

Należy przypomnieć, że przepisy dotyczące zgody na mocy RODO mają zastosowanie w kontekście przepisów o prywatności i łączności elektronicznej. W związku z tym EROD uważa, że konieczność uzyskania rzeczywistej dobrowolnej zgody powinna uniemożliwiać usługodawcom stosowanie nieuczciwych praktyk, takich jak stosowanie praktyki „zaakceptuj lub odrzuć" uzależniającej dostęp do usług i funkcji od zgody użytkownika na przechowywanie informacji lub od uzyskania dostępu do informacji już przechowywanych w urządzeniu końcowym użytkownika (tzw. „cookie walls")[5].

EROD podkreśla potrzebę włączenia do rozporządzenia w sprawie prywatności i łączności elektronicznej wyraźnego przepisu ustanawiającego ten zakaz, aby umożliwić użytkownikom akceptację lub odmowę profilowania. Ci sami usługodawcy powinni zatem proponować użytkownikom uczciwe alternatywy. Zasady te powinny mieć jednakowe zastosowanie do wszystkich usługodawców, niezależnie od sektora ich działalności lub ich obecnego modelu finansowania (zob. motyw 21aa stanowiska Rady).

Pomiar liczby odbiorców powinien ograniczać się do nieinwazyjnych praktyk, co do których nie ma podejrzenia, że stwarzają zagrożenia dla prywatności użytkowników.

Stanowisko Rady wprowadza nowy wyjątek dotyczący pomiaru liczby odbiorców, zgodnie z sugestią Grupy Roboczej Art. 29[6]. Proponowany przez Radę wyjątek dotyczący pomiaru liczby odbiorców jest jednak sformułowany zbyt szeroko i mógłby prowadzić do zbyt szerokiej interpretacji możliwego zakresu wyjątku, a tym samym do obniżenia stopnia ochrony urządzeń użytkowników końcowych.

---

[3] Oświadczenie Grupy Roboczej Art. 29 dot. szyfrowania i jego wpływu na ochronę osób fizycznych w związku z przetwarzaniem ich danych osobowych w UE, 11 kwietnia 2018 r., dostępne pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

[4] A także powiązane motywy (20aaaa i 21aa stanowiska Rady).

[5] Jak to wcześniej stwierdziła EROD w oświadczeniu dotyczącym zmian rozporządzenia w sprawie prywatności i łączności elektronicznej, przyjętym w dniu 25 maja 2018 r., dostępnym pod adresem: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_pl.pdf i w swoich wytycznych 05/2019, dotyczących zgody na mocy rozporządzenia 2016/679, pkt 39, dostępnych pod adresem: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_pl.pdf.

[6] Zob. również Opinia 04/2012 w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody (WP 194), s. 10-11. Dostępne pod adresem: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_pl.pdf.

W związku z tym EROD podkreśla, że wyjątek dotyczący pomiaru liczby odbiorców powinien być ograniczony do analizy niskiego poziomu niezbędnej do analizy wykonania usługi żądanej przez użytkownika i wyłącznie do dostarczania danych statystycznych operatorowi usług oraz musi zostać wprowadzony przez operatora lub jego podmioty przetwarzające. W związku z tym ta operacja przetwarzania nie może prowadzić, samodzielnie ani w połączeniu z innymi rozwiązaniami w zakresie śledzenia, do wyodrębnienia lub tworzenia profili użytkowników przez dostawcę usługi czy też innych administratorów danych. Ponadto usługa pomiaru liczby odbiorców nie powinna umożliwiać gromadzenia informacji nawigacyjnych dotyczących użytkowników na różnych stronach internetowych lub w różnych aplikacjach i powinna obejmować łatwo dostępny dla użytkownika mechanizm braku zgody na jakiekolwiek zbieranie danych.

Skuteczny sposób uzyskiwania zgody przez strony internetowe i aplikacje mobilne (art. 4a)

EROD uważa, że rozporządzenie w sprawie prywatności i łączności elektronicznej powinno poprawić obecną sytuację, oddając użytkownikom kontrolę i rozwiązując kwestię „zmęczenia wyrażaniem zgody". Art. 4a powinien pójść dalej i zobowiązywać przeglądarki i systemy operacyjne do wprowadzenia łatwo dostępnego dla użytkownika i skutecznego mechanizmu umożliwiającego administratorom uzyskanie zgody w celu stworzenia równych warunków działania dla wszystkich podmiotów. Zakres rozporządzenia powinien również wyraźnie obejmować dostawców przeglądarek i systemów operacyjnych.

Ustawienia prywatności powinny domyślnie zachowywać prawo do ochrony danych osobowych i integralności urządzeń użytkowników oraz umożliwić wyrażanie i wycofywanie zgody w sposób łatwy, wiążący i egzekwowalny wobec wszystkich stron.

Dalsze przetwarzanie do celów zgodnych z pierwotnym celem (art. 6c i art. 8 ust. 1 lit. g))

W odniesieniu do toczących się dyskusji na temat dalszego przetwarzania metadanych/danych pochodzących z łączności elektronicznej zbieranych za pomocą plików cookie i podobnych technologii, EROD ponownie wyraża swoje poparcie dla podejścia przyjętego w rozporządzeniu w sprawie prywatności i łączności elektronicznej, pierwotnie zaproponowanego przez Komisję Europejską i przyjętego przez Parlament Europejski, opartego na ogólnym zakazie i przewidującego wąskie wyjątki oraz wykorzystanie zgody. Dalsze przetwarzanie do celów zgodnych z pierwotnym celem wiąże się z ryzykiem osłabienia ochrony zapewnianej przez rozporządzenie w sprawie prywatności i łączności elektronicznej, zwłaszcza w odniesieniu do przetwarzania metadanych pochodzących z łączności elektronicznej, poprzez zezwolenie na przetwarzanie w dowolnym celu, który w ocenie dostawcy usług spełnia warunek zgodności, podczas gdy prawodawca wyraźnie dążył do ograniczenia ich wykorzystania do konkretnych celów w przypadku braku zgody. EROD pragnie podkreślić, że wyżej wspomniane dane mogą być nadal przetwarzane bez zgody i bez stwarzania ryzyka dla użytkowników po ich zanonimizowaniu.

Przyszła rola organów nadzorczych i EROD oraz mechanizm współpracy (art. 18-20)

EROD przypomina, że w celu zagwarantowania równych warunków działania na jednolitym rynku cyfrowym niezbędne jest zapewnienie zharmonizowanej interpretacji i egzekwowania wszystkich przepisów rozporządzenia w sprawie prywatności i łączności elektronicznej dotyczących przetwarzania danych w całej UE.

Nadzór nad przepisami dotyczącymi prywatności zawartymi w rozporządzeniu w sprawie prywatności i łączności elektronicznej należy powierzyć właściwym organom nadzorczym określonym w RODO w celu dalszego wspierania spójności.

EROD pragnie przypomnieć, że istnieje wyraźne powiązanie kompetencji między organami krajowymi właściwymi na mocy obowiązującej dyrektywy o prywatności i łączności elektronicznej a organami ochrony danych. Przepisy przyszłego rozporządzenia w sprawie prywatności i łączności elektronicznej dotyczące ochrony prywatności nie powinny być stosowane w oderwaniu, ponieważ są powiązane z przetwarzaniem danych osobowych i z RODO.

W związku z tym, w celu pogodzenia wysokiego stopnia ochrony danych osobowych oraz pewności prawnej i proceduralnej, nadzór nad przepisami przyszłego rozporządzenia w sprawie prywatności i łączności elektronicznej dotyczącymi przetwarzania danych osobowych należy powierzyć organom krajowym odpowiedzialnym za egzekwowanie RODO, zgodnie z pierwotnym wnioskiem Komisji Europejskiej[7].

EROD zauważa, że w przeciwieństwie do pierwotnego wniosku Komisji Europejskiej wszystkie odniesienia do mechanizmu współpracy i spójności, przewidzianego w rozdziale VII RODO, zostały usunięte ze stanowiska Rady. Z powodów przypomnianych powyżej EROD powtarza, że jedynie pełna zgodność z ramami współpracy i spójności przewidzianymi w RODO umożliwiłaby osiągnięcie celów rozporządzenia w sprawie prywatności i łączności elektronicznej, uniknięcie fragmentacji w egzekwowaniu i stosowaniu rozporządzenia, a także zmniejszenie obciążeń dla dostawców, którzy w przeciwnym razie musieliby potencjalnie mieć do czynienia z ponad 27 organami nadzorczymi.

W przypadku gdyby właściwe organy krajowe niebędące członkami EROD musiały współdziałać z EROD, jak przewiduje obecnie stanowisko Rady, ich zdolność do terminowego przyczynienia się do spójnego stosowania rozporządzenia w sprawie prywatności i łączności elektronicznej zmniejszyłaby się ze szkodą zarówno dla gospodarki cyfrowej, jak i dla ochrony praw podstawowych.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek

ZAŁĄCZNIK: Wykaz poprzednich dokumentów sporządzonych przez EROD i Grupę Roboczą Art. 29

- Opinia 1/2009 w sprawie wniosków zmieniających dyrektywę 2002/58/WE o prywatności i łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), dostępna pod adresem: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_pl.pdf.
- Opinia 04/2012 w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody (WP 194), dostępna pod adresem: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_pl.pdf.

[7] Komisja Europejska, 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 (rozporządzenia w sprawie prywatności i łączności elektronicznej), 10 stycznia 2017 r., dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010 oraz powiązana opinia Grupy Roboczej Art. 29, dostępna pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140.

- Opinia 03/2016 w sprawie oceny i przeglądu dyrektywy o prywatności i łączności elektronicznej (WP 240), dostępna pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.
- Opinia Grupy Roboczej Art. 29 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenia w sprawie prywatności i łączności elektronicznej), dostępna pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140.
- Oświadczenie Grupy Roboczej Art. 29 dot. szyfrowania i jego wpływu na ochronę osób fizycznych w związku z przetwarzaniem ich danych osobowych w UE, Bruksela, 11 kwietnia 2018 r., dostępne pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
- Oświadczenie EROD dotyczące zmiany rozporządzenia w sprawie prywatności i łączności elektronicznej oraz jego wpływu na ochronę osób fizycznych w zakresie prywatności i poufności komunikacji, przyjęte w dniu 25 maja 2018 r., dostępne pod adresem: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_pl.pdf.
- Oświadczenie EROD 3/2019 w sprawie rozporządzenia o prywatności i łączności elektronicznej, przyjęte w dniu 13 marca 2019 r., dostępne pod adresem: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf.
- Oświadczenie EROD na temat rozporządzenia w sprawie prywatności i łączności elektronicznej oraz przyszłej roli organów nadzorczych i EROD, przyjęte w dniu 19 listopada 2020 r., dostępne pod adresem: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_pl.pdf.