EROD: Oświadczenie w sprawie interoperacyjności aplikacji służących ustalaniu kontaktów zakaźnych, oświadczenie w sprawie otwarcia granic i prawa do ochrony danych, odpowiedź do europosła Körnera w sprawie osłon kamer internetowych oraz pismo do Komitetu Europejskich Organów Nadzoru Audytowego (CEAOB)

Wtorek, 16 czerwca 2020 r.

Podczas 32. posiedzenia plenarnego, Europejska Rada Ochrony Danych przyjęła oświadczenie w sprawie interoperacyjności aplikacji do ustalania kontaktów zakaźnych, jak również oświadczenie w sprawie otwarcia granic i prawa do ochrony danych. Rada przyjęła również dwa pisma do eurodeputowanego Körnera - w sprawie szyfrowania oraz art. 25 RODO – a także pismo do CEAOB w sprawie ustaleń dotyczących amerykańskiej Rady Nadzoru Rachunkowości Spółek Publicznych (PCAOB).

EROD przyjęła oświadczenie w sprawie interoperacyjności aplikacji służących ustalaniu kontaktów zakaźnych, opierając się na Wytycznych EROD 4/2020 w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19. Oświadczenie przedstawia pogłębioną analizę kluczowych aspektów, w tym przejrzystości przetwarzania, podstawy prawnej, administrowania, praw osób, których dane dotyczą, zatrzymywania i minimalizacji danych, bezpieczeństwa informacji oraz prawidłowości danych w kontekście tworzenia interoperacyjnej sieci aplikacji, które muszą być rozpatrywane jako uzupełnienie tych wymienionych w Wytycznych EROD 4/2020.

EROD podkreśla, że udostępnianie danych o osobach, które zostały pozytywnie zdiagnozowane lub uzyskały pozytywny wynik testu, przy pomocy takich interoperacyjnych aplikacji, powinno się odbywać wyłącznie na podstawie dobrowolnego działania użytkownika. Udzielanie informacji osobom, których dane dotyczą oraz posiadanie kontroli nad swoimi danymi, zwiększy ich zaufanie do rozwiązań i ich potencjalnego wykorzystania. Cel interoperacyjności nie powinien być wykorzystywany jako argument do rozszerzenia gromadzenia danych osobowych ponad to, co jest niezbędne.

Ponadto aplikacje do ustalania kontaktów zakaźnych muszą być elementem kompleksowej strategii zdrowia publicznego, mającej na celu zwalczanie pandemii, obejmującej m.in. badania i dalsze ustalanie kontaktów zakaźnych tradycyjnymi metodami dla poprawy efektywności przeprowadzanych działań.

Zapewnienie interoperacyjności jest nie tylko technicznie trudne, a czasem niemożliwe bez nieproporcjonalnych kompromisów, ale także prowadzi do potencjalnie zwiększonego ryzyka ochrony danych. Dlatego administratorzy muszą zapewnić skuteczność i proporcjonalność środków oraz muszą ocenić, czy za pomocą alternatywnego środka, który jest mniej inwazyjny, można osiągnąć ten sam cel.

EROD przyjęła oświadczenie w sprawie przetwarzania danych osobowych w kontekście ponownego otwarcia granic Schengen w następstwie pandemii COVID-19. Środki pozwalające na bezpieczne ponowne otwarcie granic, które są obecnie przewidywane lub wdrażane przez państwa członkowskie, obejmują badania na obecność COVID-19, wymóg posiadania certyfikatów wydawanych przez pracowników służby zdrowia i korzystanie z dobrowolnej

aplikacji służącej ustalaniu kontaktów zakaźnych. Większość środków wiąże się z przetwarzaniem danych osobowych.

EROD przypomina, że przepisy dotyczące ochrony danych nadal obowiązują i pozwalają na skuteczne reagowanie na pandemię, chroniąc jednocześnie podstawowe prawa i wolności. EROD podkreśla, że przetwarzanie danych osobowych musi być niezbędne i proporcjonalne, a stopień ochrony powinien być spójny w całym Europejskim Obszarze Gospodarczym. W oświadczeniu EROD wzywa państwa członkowskie do przyjęcia wspólnego europejskiego podejścia przy podejmowaniu decyzji, w których przetwarzanie danych osobowych w tym kontekście jest niezbędne.

Oświadczenie dotyczy również zasad RODO, na które państwa członkowskie muszą zwrócić szczególną uwagę podczas przetwarzania danych osobowych w kontekście ponownego otwarcia granic. Obejmują one zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizację danych, ograniczenie przechowywania, bezpieczeństwo danych a także uwzględnianie ochrony danych w fazie projektowania oraz domyślną ochronę danych. Ponadto decyzja zezwalająca na wjazd do kraju powinna opierać się nie tylko na technologiach zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach. Za każdym razem tego typu decyzje powinny podlegać odpowiednim zabezpieczeniom, które powinny zawierać szczegółowe informacje dla osoby, której dane dotyczą oraz prawo do interweniowania w celu wyrażenia swojego punktu widzenia, uzyskania wyjaśnienia decyzji podjętej po takiej ocenie oraz zakwestionowania decyzji. Narzędzia zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach nie powinny mieć zastosowania do dzieci.

EROD podkreśla wreszcie znaczenie uprzednich konsultacji z właściwymi organami nadzorczymi na poziomie krajowym, gdy państwa członkowskie zamierzają przetwarzać dane osobowe w tym kontekście.

EROD przyjęła odpowiedź na pismo posła do Parlamentu Europejskiego Moritza Körnera w sprawie znaczenia zakazów szyfrowania w krajach trzecich dla oceny poziomu ochrony danych w przypadku przekazywania danych osobowych do krajów, w których te zakazy funkcjonują. Według EROD każdy zakaz szyfrowania lub przepisy osłabiające szyfrowanie poważnie naruszyłyby przestrzeganie obowiązków w zakresie bezpieczeństwa wynikających z RODO mających zastosowanie do administratorów i podmiotów przetwarzających, zarówno w państwie trzecim, jak i w Europejskim Obszarze Gospodarczym. Środki bezpieczeństwa są jednym z elementów, które Komisja Europejska musi wziąć pod uwagę przy ocenie odpowiedniego stopnia ochrony w kraju trzecim.

Drugi list do posła do Parlamentu Europejskiego Körnera dotyczy osłon kamer internetowych. Eurodeputowany Körner podkreślił, że ta technologia może pomóc w zachowaniu zgodności z RODO i zasugerował, że nowe laptopy powinny być w nie wyposażone. W swojej odpowiedzi Rada wyjaśnia, że chociaż producenci laptopów powinni być zachęcani do uwzględnienia prawa do ochrony danych przy opracowywaniu i projektowaniu takich produktów, nie są oni odpowiedzialni za przetwarzanie danych w ramach tych produktów, a RODO nie ustanawia zobowiązań prawnych dla producentów, chyba że działają oni również jako administratorzy lub podmioty przetwarzające.

Administratorzy danych muszą ocenić ryzyko związane z każdym przetwarzaniem i wybrać odpowiednie zabezpieczenia zgodne z RODO, w tym ochronę prywatności w fazie projektowania i domyślną ochronę danych zapisaną w art. 25 RODO.

Wreszcie **EROD przyjęła list do Komitetu Europejskich Organów Nadzoru Audytowego** (CEAOB). EROD otrzymała propozycję od CEAOB, który skupia krajowe organy nadzoru audytowego na poziomie europejskim, dotyczącą współpracy i wymiany informacji zwrotnych na temat negocjacji projektów ustaleń administracyjnych dotyczących przekazywania danych do amerykańskiej Rady Nadzoru Rachunkowości Spółek Publicznych (PCAOB). EROD z zadowoleniem przyjmuje ten wniosek i wskazuje, że istnieje możliwość przeprowadzenia wymiany informacji z CEAOB w celu wyjaśnienia wszelkich potencjalnych pytań dotyczących wymogów ochrony danych związanych z takimi ustaleniami w świetle Wytycznych EROD 2/2020 w sprawie art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 do celów przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG. Wymiana może również obejmować PCAOB, jeżeli CEAOB i jego członkowie uznają to za korzystne dla ich pracy nad tymi uzgodnieniami.