

Apel Związku Cyfrowa Polska o ścisłą współpracę transatlantycką na polu technologii cyfrowych w obliczu rosnącego zagrożenia dla kraju i Europy

W obliczu nieusprawiedliwionej i niesprowokowanej napaści Federacji Rosyjskiej na Ukrainę oraz obaw związanych z rosyjską próbą ekspansji poprzez agresję, polska branża cyfrowa i nowoczesnych technologii pragnie przypomnieć o szczególnym znaczeniu, współpracy Unii Europejskiej, w tym Polski, ze Stanami Zjednoczonymi Ameryki.

Jako sektor świadomy zagrożeń, przed którymi stoi Europa i jej partnerzy, apelujemy by obie strony relacji UE-USA podjęły zdecydowane działania na rzecz rozwiązania najistotniejszych problemów, z którymi przychodzi nam się mierzyć. Jesteśmy przekonani, że w uporaniu się z nimi na drodze kooperacji transatlantyckiej szczególnego znaczenia nabierają dziś działania podejmowane w ramach Rady ds. Handlu i Technologii (TTC) powołanej w czerwcu 2021 r. podczas szczytu UE-USA oraz pogłębianie współpracy m.in. na polu opracowywania i przyjmowania wspólnych standardów technologicznych w kluczowych obszarach, takich jak sztuczna Inteligencja (AI), internet rzeczy (IoT), cyberbezpieczeństwo, ale również w sferze praw człowieka.

Dla Polski - państwa, w którym aktywność biznesu wywodzącego się ze Stanów Zjednoczonych ma wieloletnią tradycję i wnosi niesłychanie wiele w rozwój sektora ICT, umacnianie tej współpracy ma szczególnie istotny wymiar. Wojna wywołana rosyjską agresją, trwająca tuż za granicami UE sprawia, że konieczne jest odejście od biurokratycznej, ściśle kontynentalnej perspektywy i zupełnie nowe spojrzenie na bezpieczeństwo przetwarzania danych, dla zapewnienia którego granice UE mogą okazać się niewystarczające. Transfer danych za oceany to szansa, by zwiększyć bezpieczeństwo zarówno państw UE, jak i pojedynczych podmiotów infrastruktury krytycznej. Pamiętać należy, że USA to główny gwarant naszego bezpieczeństwa w NATO, a bezpieczeństwo to nabiera dziś również wymiaru cyfrowego..

Stoimy na stanowisku, że pogłębienie współpracy transatlantyckiej w zakresie bezpieczeństwa ma kluczowe znaczenie. Zarówno w Europie, jak i w Stanach Zjednoczonych stale wzrasta liczba incydentów bezpieczeństwa. Przeciwdziałać należy zagrożeniom związanym z cyberatakami, mającymi swoje źródło m.in. w Chińskiej Republice Ludowej i Federacji Rosyjskiej. W przeciwnym wypadku narażeni będziemy na sytuacje takie, jak ta znana z ubiegłego roku, gdy grupa cyberprzestępców z Chin dokonała cyberatak na serwery firmy Microsoft, który wpłynął na podmioty na całym świecie - również w UE, gdzie skutki ataku odczuł Europejski Urząd Nadzoru Bankowego. Należy też bezwzględnie

rozwinąć współpracę w obszarze przeciwdziałania dezinformacji i zagrożeniom hybrydowym w ramach istniejącego cyberdialogu na linii UE-USA.

Nie bez znaczenia dla przyszłości tej współpracy jest fakt, że Stany Zjednoczone krytycznie podchodzą do europejskich planów regulacji rynku cyfrowego, które wpłyną na działalność amerykańskich korporacji technologicznych. Przedstawione przez KE projekty mające na celu regulację platform internetowych przewidują listę obowiązków i ograniczeń dotyczących największych - w znacznej większości amerykańskich - podmiotów. Ponadto, niektóre obowiązki w zawartym w czwartek (24 marca) wstępnym porozumieniu politycznym w sprawie aktu o rynkach cyfrowych (DMA) mogą mieć niepożądane konsekwencje dla bezpieczeństwa i ochrony danych użytkowników oraz potencjalnie lekceważyć zasady prawa własności intelektualnej. Z przykrością odnotowujemy próby narzucania narodowych standardów na arenie rynku cyfrowego Europy przez niektóre państwa członkowskie UE, szczególnie gdy mają one wyraźnie dyskryminacyjny i antyamerykański charakter, tak jak miało to miejsce np. podczas próby przeforsowania krajowych standardów przetwarzania w chmurze przez prezydencję francuską.

Doskonale rozumiemy, że negocjacje UE-USA nad nowym porozumieniem dot. transferu i zarządzania danymi osobowymi są trudnym i czasochłonnym zadaniem. Jesteśmy jednak zdania, że prace te nie mogą przebiegać przy przyjętym założeniu, że trwać będą jeszcze latami, tak jak ma to miejsce obecnie. W lipcu 2020 r. Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał wyrok unieważniający umowę Privacy Shield (Tarczę Prywatności), na mocy której legalne było przesyłanie i magazynowanie danych, np. europejskich użytkowników portali społecznościowych na terytorium USA. TSUE uzasadnił swoją decyzję faktem, że amerykańskie prawo przewiduje zbyt duży dostęp służb specjalnych do gromadzonych danych. Co więcej, kolejne organy ochrony danych w państwach członkowskich UE kwestionują wewnętrzne zapisy dot. ochrony prywatności firm amerykańskich. Postąpił tak np. austriacki Urząd Ochrony Danych Osobowych. Mimo tej napiętej, niesprzyjającej współpracy sytuacji i politycznych zapowiedzi, nie opracowano wciąż nowej wersji stosownej umowy. Jest ona jednak bezwzględnie i pilnie potrzebna. Brak zgody co do zasad polityki prywatności ogranicza możliwość wymiany danych, rozwój usług (m.in. chmurowych), a także zwiększa koszty działalności firm branży cyfrowej.

Wzywamy zarówno rząd Polski jak i Komisję Europejską do podjęcia zdecydowanych i intensywnych działań na rzecz uregulowania stosunków handlowych UE-USA w sferze nowoczesnych technologii w sposób sprzyjający owocnemu i obustronnie korzystnemu przepływowi innowacji i zdobyczy ery cyfrowej. Jesteśmy przekonani, że stabilna i podparta solidną podstawą prawną współpraca transatlantycka w sferze cyfrowej jest warunkiem koniecznym dla zapewnienia bezpieczeństwa Polski i Europy. Przypominamy o fundamentalnym znaczeniu przepływu danych dla rozwoju nowoczesnej gospodarki i deklarujemy chęć i gotowość, by wspierać naszych liderów w opracowaniu niezbędnych ram prawnych.