

CNIL: zagrożenia związane z europejskim certyfikatem  
umożliwiającym zagranicznym organom dostęp do wrażliwych  
danych

# CNIL: zagrożenia związane z europejskim certyfikatem umożliwiającym zagranicznym organom dostęp do wrażliwych danych

Posted on 2024-09-30

Według francuskiego organu nadzorczego (CNIL) w obecnym stanie europejski system certyfikacji usług w chmurze (EUCS) nie pozwala już dostawcom na wykazanie, że chronią oni przechowywane dane przed niepożądanym dostępem. CNIL apeluje o zwiększenie

CNIL: zagrożenia związane z europejskim certyfikatem  
umożliwiającym zagranicznym organom dostęp do wrażliwych  
danych

poziomu ochrony danych osobowych w tym certyfikacie poprzez ponowne wprowadzenie odpowiednich gwarancji.

# Dane wrażliwe, które muszą być szczególnie chronione

CNIL uważa, że dane przechowywane przez firmę podlegającą prawu pozaeuropejskiemu, jak ma to miejsce w przypadku dostawców usług hostingowych, których spółki macierzyste znajdują się w Stanach Zjednoczonych, mogą być narażone na ryzyko konieczności ujawnienia danych organom publicznym tego kraju. Ryzyko to jest ogólnie uważane za ograniczone, szczególnie w przypadku danych niewrażliwych powierzonych dostawcom usług z siedzibą w krajach zapewniających odpowiedni stopień ochrony danych. Dotyczy to w szczególności Stanów Zjednoczonych, które są krajem zapewniającym odpowiedni stopień ochrony danych od czasu decyzji Komisji Europejskiej z dnia 10 lipca 2023 r. (na warunkach określonych w Ramach ochrony danych UE-USA). Wzmocniona ochrona jest jednak wymagana w przypadku przetwarzania najbardziej wrażliwych danych (np. dużych baz danych dotyczących zdrowia, danych dotyczących przestępstw lub danych dotyczących nieletnich), w przypadku których dane przechowywane w Unii Europejskiej nie powinny być narażone na ryzyko nieuprawnionego dostępu ze strony organów w państwach trzecich.

W takich przypadkach CNIL zaleca korzystanie z usług dostawcy, który podlega wyłącznie prawu europejskiemu i zapewnia odpowiedni poziom ochrony. We Francji, w przypadku usług przetwarzania w chmurze, certyfikat SecNumCloud wydany przez Agence nationale de la sécurité des systèmes d'information (ANSSI) obejmuje to kryterium, chroniąc dane przed dostępem organów zagranicznych.

CNIL: zagrożenia związane z europejskim certyfikatem  
umożliwiającym zagranicznym organom dostęp do wrażliwych  
danych

# Niedociągnięcia i zagrożenia związane z europejskim projektem certyfikacji EUCS

Możliwość zapewnienia, w przypadku najbardziej wrażliwych operacji przetwarzania, że podmiot przechowujący dane nie podlega przepisom pozaeuropejskim, nie jest już uwzględniona w projekcie EUCS dotyczącym europejskiej certyfikacji bezpieczeństwa usług w chmurze, pilotowanym przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). CNIL podkreśla, że od dawna zaleca, aby najbardziej wrażliwe bazy danych osobowych (takie jak krajowy system danych zdrowotnych (SNDS) lub dane dotyczące nieletnich), były chronione we Francji przed ich ujawnieniem organom publicznym w krajach trzecich. CNIL wzywa do włączenia, na zasadzie opcjonalnej, kryteriów „odporności” na przepisy pozaeuropejskie, które mogłyby być inspirowane kwalifikacjami SecNumCloud już obowiązującymi we Francji, do europejskiego systemu certyfikacji EUCS, w celu zapewnienia najwyższej ochrony przetwarzania najbardziej wrażliwych danych osobowych dla europejskich podmiotów przemysłowych.

## Źródło:

komunikat francuskiego organu nadzorczego CNIL