

FIRMY Z USA PODPISAŁY UMOWĘ PRIVACY SHIELD

Porozumienie Privacy Shield wynikało z braku wystarczających rozwiązań oraz pokrycia zakresu tematycznego przy przesyłaniu informacji o klientach firm amerykańskich na terenie Europy. Nowa umowa zastąpiła działającą do tej pory umowę Safe Harbor, która nie zapewniała odpowiedniej ochrony dla danych osobowych obywateli Unii Europejskiej.

Privacy Shield podpisały do tej pory łącznie 42 firmy działające na terenie Europy, które swoją główną siedzibę mają w Stanach Zjednoczonych. Wśród firm, które podpisały umowę znajduje się m.in. Microsoft, Workday Inc. czy Salesforce.com. Jak informowaliśmy na [lamach Cyberdefence24](#) w lipcu tego roku. Porozumienie sprostą problemom, jakie wynikały z omijania przez niektóre firmy zapisów porozumienia, co doprowadziło do sytuacji, w których dane udostępniane organom ścigania nie były pełne. Firmy oraz administracja przyjęły zmiany pozytywnie, głównie ze względu na wysoki poziom zabezpieczeń zarówno dla obywateli europejskich jak i amerykańskich. Ekspertcy pochwalili również przejrzystość prawa w przypadku zarządzania danymi obywateli.

Według osób odpowiedzialnych za wprowadzenie zmian w ramach Privacy Shield, obecnie na rozpatrzenie aplikacji w ramach porozumienia czeka 200 firm. Jednak możemy mieć pewność, że niedługo więcej przedsiębiorstw zainteresuje się tym tematem. Do tej pory ponad 4 tys. firm posiadało certyfikat i działa w ramach umowy Safe Harbor, jednak w październiku zeszłego roku Europejski Trybunał Sprawiedliwości stwierdził niezgodność porozumienia z prawem europejskim. To spowodowało, że firmy, które nie posiadały innych certyfikatów uprawniających ich do działania na mocy tego porozumienia, nie mogły prowadzić działań poza granicami kraju, lub musiały zdobyć inne podobne certyfikaty.

Departament Handlu Stanów Zjednoczonych uruchomił rejestrację oraz wydawanie certyfikatów na początku tego miesiąca, w przypadku nie przestrzegania zapisów umowy firmy czekają wysokie sankcje. Nie jest znany dokładny rozmiar sankcji, w dokumencie pojawia się jedynie zdanie „sankcje muszą być wystarczająco rygorystyczne, w celu zapewnienia przestrzegania zapisów przez organizacje”.

Czytaj też: [CERT: Raport o stanie cyberbezpieczeństwa Polski](#)