REPUBLIKA FRANCUSKA

Premier

Projekt rozporządzenia dotyczącego ochrony danych strategicznych i wrażliwych na rynku przetwarzania w chmurze

Nr NOR:

Podmioty, których dotyczy rozporządzenie: *Administracje państwowe i operatorzy państwowi, grupy interesu publicznego*

Przedmiot: …

Wejście w życie: *Rozporządzenie wchodzi w życie następnego dnia po jego opublikowaniu.*

Uwaga: ….

Odniesienia: *Rozporządzenie wdraża art. 31 ustawy nr 2024-449 z dnia 21 maja 2024 r. o zabezpieczeniu i regulacji przestrzeni cyfrowej. Można się z nim zapoznać na stronie internetowej Légifrance (http://www.legifrance.gouv.fr).*

Premier,

W sprawozdaniu z dnia XX,

uwzględniając rozporządzenie (UE) 2019/881 Parlamentu Europejskiego i Rady z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz w sprawie certyfikacji cyberbezpieczeństwa technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013;

uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/1535 z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego;

uwzględniając kodeks obrony, w szczególności art. D. 3126-2;

uwzględniając rozporządzenie nr 2005-1516 z dnia 8 grudnia 2005 r. w sprawie elektronicznej wymiany informacji między użytkownikami a organami administracyjnymi oraz między organami administracyjnymi, w szczególności jego art. 9,

uwzględniając ustawę nr 2016-1321 z dnia 7 października 2016 r. o Republice Cyfrowej, w szczególności jej art. 16;

uwzględniając ustawę nr 2024-449 z dnia 21 maja 2024 r. w sprawie zabezpieczenia i regulacji przestrzeni cyfrowej, w szczególności jej art. 31;

uwzględniając rozporządzenie nr 2014-445 z dnia 30 kwietnia 2014 r. w sprawie zadań i organizacji Dyrekcji Generalnej ds. Bezpieczeństwa Wewnętrznego;

uwzględniając rozporządzenie nr 2015-350 z dnia 27 marca 2015 r., z późniejszymi zmianami, w sprawie kwalifikacji produktów związanych z bezpieczeństwem i dostawców usług zaufania dla potrzeb systemów informatycznych w zakresie bezpieczeństwa;

uwzględniając notyfikację nr XX wysłaną do Komisji Europejskiej w dniu XXX;

po konsultacji z Radą Stanu (sekcja administracji),

rozporządza, co następuje:

Artykuł 1

Wykaz grup interesu publicznego, o którym mowa w art. 31 lit. I ww. ustawy z dnia 21 maja 2024 r., obejmuje:

- grupę interesu publicznego znaną jako „Agencja Zdrowia Cyfrowego (ANS)”;
- grupę interesu publicznego znaną jako „Krajowa Agencja Badań nad AIDS (ANRS)”;
- grupę interesu publicznego znaną jako „Agencja ds. Promocji Kształcenia i Wymiany Edukacyjnej i Naukowej”;
- grupę interesu publicznego „Centrum Bezpiecznego Dostępu do Danych (CASD)”;
- grupę interesu publicznego „Centrum Zasobów na rzecz Zapobiegania Radykalizacji”;
- grupę interesu publicznego „Krajowa Szkoła Weterynaryjna”;
- grupę interesu publicznego „Grupa Interesu Publicznego ds. Wysokoaktywnych Zamkniętych Źródeł Promieniotwórczych (GIP SOURCES HA)”;
- grupę interesu publicznego „Krajowy System Rejestracji Zapotrzebowania na Mieszkania Socjalne (GIP SNE)”;
- grupę interesu publicznego „Modernizacja deklaracji społecznych (GIP-MDS)”;
- grupę interesu publicznego „Obserwatorium Nauki i Technologii”.

Artykuł 2

I - W celu zastosowania art. 31 ww. ustawy z dnia 21 maja 2024 r. prywatny usługodawca musi wdrożyć następujące kryteria bezpieczeństwa i ochrony danych:

- udokumentowaną politykę bezpieczeństwa informacji i zarządzania ryzykiem obejmującą łańcuch podwykonawstwa;
- bezpieczny system zarządzania zasobami ludzkimi dla personelu zaangażowanego w świadczenie usługi;
- narzędzia i procedury bezpiecznego zarządzania sprzętem wdrażającym usługę i systemy informatyczne;
- fizyczne, środowiskowe i logiczne środki bezpieczeństwa, takie jak stosowanie mechanizmów szyfrowania, kontrola dostępu i zarządzanie tożsamością użytkownika;
- procedury zarządzania incydentami dotyczącymi bezpieczeństwa informacji oraz środki zapewnienia ciągłości działania;
- środki w celu zapewnienia zgodności z przepisami prawnymi obowiązującymi we Francji i środkami ochrony danych, w szczególności umownymi, dla przetwarzanych lub przechowywanych danych przeciwko wszelkim dostępom organów publicznych państw trzecich, które nie są upoważnione na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, w tym w szczególności warunki regulujące posiadanie kapitału i praw głosu w spółce usługodawcy oraz ustanowienie usługodawcy i wszelkich podwykonawców.

Ramy opracowane przez francuską Agencję ds. Cyberbezpieczeństwa na warunkach określonych w ww. rozporządzeniu z dnia 27 marca 2015 r. ustanawiają wymogi odnoszące się do tych kryteriów. Konsultacje niezbędne do stworzenia i rozwoju tych ram odniesienia dla państwowego systemu informacyjnego prowadzone są w porozumieniu z Międzyresortową Dyrekcją Cyfrową.

II - W celu spełnienia wymogów w zakresie ochrony i bezpieczeństwa danych, o których mowa w art. 31 ust. I ww. ustawy z dnia 21 maja 2024 r., zainteresowane administracje mają prawo do odwołania się do usług przetwarzania w chmurze świadczonych przez kwalifikowanego prywatnego usługodawcę, udzielanych na warunkach określonych w rozdziale III wspomnianego rozporządzenia z dnia 27 marca 2015 r. i spełniające kryteria, o których mowa w pkt I niniejszego artykułu, lub europejskiej certyfikacji na co najmniej równoważnym poziomie.

III - Operacyjne i komunikacyjne systemy informacyjne, naukowe i techniczne systemy informacyjne, oraz systemy informatyczne, które wykorzystują, wymagają lub zawierają niejawne media lub informacje obejmujące obronny system informacyjno-komunikacyjny, a także systemy informacyjno-komunikacyjne obsługiwane przez służby, o których mowa w art. D. 3126-2 kodeksu obrony i art. 1 wyżej wymienionego rozporządzenia z dnia 30 kwietnia 2014 r., są wyłączone z zakresu stosowania niniejszego artykułu.

Artykuł 3

I - Jeżeli w dniu wejścia w życie art. 31 ww. ustawy z dnia 21 maja 2024 r. administracja zainicjowała już projekt spełniający warunki określone w ww. artykule i korzystający z usługi chmury obliczeniowej świadczonej przez prywatnego usługodawcę, który nie spełnia kryteriów bezpieczeństwa i ochrony danych określonych w art. 2 niniejszego rozporządzenia, może ona wnioskować, zgodnie z procedurami określonymi w zarządzeniu Prezesa Rady Ministrów, o odstępstwo od obowiązków określonych w tym samym artykule.

Odstępstwo to nie może przekraczać 18 miesięcy, jeżeli we Francji dostępna jest dopuszczalna oferta usług przetwarzania w chmurze w rozumieniu pkt II niniejszego artykułu. Jeżeli w dniu złożenia wniosku o odstępstwo we Francji nie jest dostępna dopuszczalna oferta chmury obliczeniowej, odstępstwo nie może przekroczyć jednego roku przed ewentualnym złożeniem nowego wniosku.

Odstępstwo to jest przyznawane na mocy uzasadnionej decyzji ministra odpowiedzialnego za projekt i zatwierdzane przez premiera.

Jest ona podawana do wiadomości publicznej na warunkach określonych w księdze III kodeksu public relations.

II – Ocena dopuszczalności oferty usług przetwarzania w chmurze w rozumieniu art. 31 ust. III ustawy z dnia 21 maja 2024 r., o której mowa powyżej, opiera się na następujących kryteriach:

- potrzeba funkcjonalna, którą oferta jest w stanie zaspokoić, z uwzględnieniem zadań danej administracji;
- warunki finansowe;
- operacyjne i techniczne warunki bezpieczeństwa i ochrony danych przetwarzanych przez dostawcę oferty zgodnie z wymogami określonymi w art. 2 niniejszego rozporządzenia;
- warunki zakończenia umowy i gwarancje odwracalności;
- warunki kontroli, trwałości i niezależności w rozumieniu art. 16 ww. ustawy z dnia 7 października 2016 r.

Sporządzono dn.

Z upoważnienia Premiera: