REPUBBLICA FRANCESE

Il Primo ministro

Progetto di decreto sulla protezione dei dati strategici e sensibili nel mercato del cloud computing

NOR:

Gruppo target: *Amministrazioni statali e operatori, gruppi di interesse pubblico*

Oggetto: …

Entrata in vigore*: il decreto entra in vigore il giorno successivo alla sua pubblicazione.*

Nota informativa: ….

Riferimenti: *il decreto attua l'articolo 31 della legge n. 2024-449 del 21 maggio 2024 sulla messa in sicurezza e la regolamentazione dello spazio digitale. Può essere consultato sul sito web di Légifrance (http://www.legifrance.gouv.fr).*

Il Primo ministro,

sulla relazione di XX,

visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013;

vista la direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione;

visto il codice della difesa, in particolare l'articolo D. 3126-2;

vista l'ordinanza n. 2005-1516 dell'8 dicembre 2005 relativa agli scambi elettronici tra utenti e autorità amministrative e tra le autorità amministrative stesse, in particolare l'articolo 9;

vista la legge n. 2016-1321 del 7 ottobre 2016 per una Repubblica digitale, in particolare l'articolo 16;

vista la legge n. 2024-449 del 21 maggio 2024 sulla messa in sicurezza e la regolamentazione dello spazio digitale, in particolare l'articolo 31;

visto il decreto n. 2014-445 del 30 aprile 2014 sui compiti e l'organizzazione della Direzione generale della sicurezza interna;

visto il decreto n. 2015-350 del 27 marzo 2015, e successive modifiche, sulla qualificazione dei prodotti di sicurezza e dei prestatori di servizi fiduciari per le esigenze di sicurezza dei sistemi informativi;

vista la notifica n. XX inviata alla Commissione europea il XXX;

sentito il parere del Consiglio di Stato (Sezione Amministrativa),

Decreta:

Articolo 1

L'elenco dei gruppi di interesse pubblico di cui all'articolo 31, paragrafo I, della citata legge del 21 maggio 2024 comprende:

- il gruppo di interesse pubblico noto come «Agenzia per la salute digitale (ANS)»;
- il gruppo di interesse pubblico noto come «Agenzia nazionale per la ricerca sull'AIDS (ANRS)»;
- il gruppo di interesse pubblico noto come «Agenzia per la promozione della formazione e dello scambio nel settore dell'istruzione e della scienza»;
- il gruppo di interesse pubblico «Centro per l'accesso sicuro ai dati (CASD)»;
- il gruppo di interesse pubblico «Centro risorse per la prevenzione della radicalizzazione»;
- il gruppo di interesse pubblico «Scuola veterinaria nazionale»;
- il gruppo di interesse pubblico «Gruppo di interesse pubblico sulle sorgenti radioattive sigillate ad alta attività (GIP SOURCES HA)»;
- il gruppo di interesse pubblico «Sistema nazionale di registrazione della domanda di alloggi sociali (GIP SNE)»;
- il gruppo di interesse pubblico «Modernizzazione delle dichiarazioni sociali (GIP-MDS)»;
- il gruppo di interesse pubblico «Osservatorio della scienza e della tecnologia».

Articolo 2

I - Ai fini dell'applicazione dell'articolo 31 della citata legge del 21 maggio 2024, il prestatore di servizi privato deve attuare i seguenti criteri di sicurezza e protezione dei dati:

- una politica documentata di sicurezza delle informazioni e di gestione dei rischi che comprenda la catena di subappalto;
- un sistema sicuro di gestione delle risorse umane per il personale coinvolto nella prestazione del servizio;
- strumenti e procedure per la gestione sicura delle apparecchiature che implementino il servizio e i sistemi informativi;
- misure di sicurezza fisiche, ambientali e logiche, come l'uso di meccanismi di crittografia, il controllo degli accessi e la gestione dell'identità degli utenti;
- procedure di gestione degli incidenti relativi alla sicurezza delle informazioni e misure di continuità operativa;
- le misure di conformità alle disposizioni legali vigenti in Francia e le misure di protezione dei dati, in particolare quelle contrattuali, per i dati trattati o memorizzati contro qualsiasi accesso da parte di autorità pubbliche di paesi terzi non autorizzate dal diritto dell'Unione europea o dal diritto di uno Stato membro, comprese in particolare le condizioni che disciplinano la partecipazione al capitale e i diritti di voto nella società del fornitore di servizi e lo stabilimento del fornitore di servizi e di eventuali subappaltatori.

Un quadro, sviluppato dall'Agenzia francese per la cibersicurezza, in base alle condizioni del suddetto decreto del 27 marzo 2015, stabilisce i requisiti relativi a tali criteri. La consultazione necessaria per la creazione e lo sviluppo di questo quadro di riferimento per il sistema informativo statale è condotta in collaborazione con la Direzione digitale interministeriale.

II - Per soddisfare i requisiti di protezione e sicurezza dei dati di cui all'articolo 31, paragrafo I, della suddetta legge del 21 maggio 2024, le amministrazioni interessate ricorrono a servizi di cloud computing forniti da un fornitore di servizi privato qualificato, aggiudicato alle condizioni di cui al capo III del suddetto decreto del 27 marzo 2015 e che soddisfa i criteri di cui al punto I del presente articolo, o di una certificazione europea di livello almeno equivalente.

III - Sono esclusi dall'ambito di applicazione del presente articolo i sistemi informativi operativi e di comunicazione, i sistemi informativi scientifici e tecnici e i sistemi informativi che coinvolgono, richiedono o contengono supporti o informazioni classificate che costituiscono il sistema informativo e di comunicazione della difesa, nonché i sistemi informativi e di comunicazione gestiti dai servizi di cui all'articolo D. 3126-2 del codice della difesa e all'articolo 1 del decreto del 30 aprile 2014 sopra citato.

Articolo 3

I - Qualora un'amministrazione abbia già avviato, alla data di entrata in vigore dell'articolo 31 della citata legge del 21 maggio 2024, un progetto che soddisfi le condizioni previste dal suddetto articolo e che utilizzi un servizio di cloud computing fornito da un fornitore di servizi privato che non attua i criteri di sicurezza e protezione dei dati definiti all'articolo 2 del presente decreto, può richiedere, secondo le modalità stabilite con decreto del presidente del Consiglio dei ministri, una deroga agli obblighi previsti dal medesimo articolo.

Tale deroga non può superare i 18 mesi in presenza di un'offerta accettabile di servizi di cloud computing, ai sensi del punto II del presente articolo, disponibile in Francia. In assenza di un'offerta cloud accettabile disponibile in Francia alla data della richiesta di deroga, la deroga non può superare un anno prima di un'eventuale nuova richiesta.

Tale deroga è concessa con decisione motivata del ministro responsabile del progetto e convalidata dal primo ministro.

Essa è resa pubblica alle condizioni previste dal libro III del codice delle relazioni pubbliche.

II – La valutazione dell'accettabilità, ai sensi dell'articolo 31, paragrafo III, della citata legge del 21 maggio 2024, di un'offerta di servizi di cloud computing si basa sui seguenti criteri:

- l'esigenza funzionale che l'offerta è in grado di soddisfare, tenendo conto dei compiti dell'amministrazione interessata;
- le condizioni finanziarie;
- le condizioni operative e tecniche di sicurezza e protezione dei dati trattati dal fornitore dell'offerta conformemente ai requisiti di cui all'articolo 2 del presente decreto;
- le condizioni di fine contratto e le garanzie di reversibilità;
- le condizioni di controllo, sostenibilità e indipendenza ai sensi dell'articolo 16 della citata legge del 7 ottobre 2016.

Redatto il,

Da parte del primo ministro: