I servizi cloud alla prova del GDPR

I servizi cloud sono, ormai, molto diffusi nelle imprese italiane che, in questo modo, ottengono diversi vantaggi:

- non immobilizzano risorse in infrastrutture ICT;
- rendono flessibile la disponibilità di risorse;
- accedono alle informazioni “anytime” e “anywhere”;
- risparmiano i costi di manutenzione delle infrastrutture ICT.

Le soluzioni cloud, nei diversi paradigmi che possono caratterizzarle, sono, dunque, molto convenienti soprattutto per le piccole e medie imprese. Tuttavia, il Regolamento Europeo sulla Protezione dei Dati Personali n. 679/2016 (GDPR) richiede un supplemento di attenzione, con riferimento agli articoli 28 (Responsabile del trattamento) e 40 (Codici di condotta) ed all’intero Capo V che disciplina il trasferimento di dati personali verso Paesi terzi e organizzazioni internazionali.

Il rapporto titolare-responsabile

L’articolo 28 disciplina il rapporto tra il titolare del trattamento dei dati personali ed il responsabile del trattamento che è, per definizione, la persona fisica o giuridica che tratta i dati personali per conto dello stesso titolare. È il soggetto, dunque, che in concreto opera sui dati personali ed effettua su di essi tutte o alcune delle operazioni (registrazione, organizzazione, conservazione, ecc.). Non c’è dubbio che tra l’impresa ed il Cloud Service Provider (CSP) esista un rapporto del tipo titolare-responsabile. Questo significa che l’impresa, quando tratta dati personali, ha alcuni obblighi nella scelta del CSP:

- verificare che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative *compliant* rispetto al GDPR;
- fornire autorizzazioni scritte sulla possibilità di avvalersi di sub-responsabili (p.e. altri CSP);
- stipulare l'accordo tramite forme contrattuali tipiche o tramite altri atti con validità giuridica;
- fornire al responsabile apposite istruzioni per il trattamento;
- specificare, nell'accordo, la durata del trattamento, la natura e la finalità, il tipo di dati personali, le categorie di interessati;
- definire con precisione gli obblighi delle parti rispetto alle previsioni normative, europee e nazionali, in materia di trattamento dei dati personali (costituzione ed aggiornamento dei registri, DPIA, gestione delle violazioni, ecc.);
- definire le "modalità di chiusura" del contratto in termini di restituzione/cancellazione al termine del rapporto contrattuale.

È necessario, dunque, trovare una soluzione agile a queste attività che possono risultare piuttosto onerose e richiedere skill non sempre presenti in azienda.

Dove sono i dati

Inoltre, il primo degli obblighi richiede una verifica preliminare di aspetti organizzativi e tecnici e, tra questi, una specifica analisi rispetto alla materiale collocazione dei dati. Un servizio cloud, sotto questo aspetto, può presentare particolari criticità perché strutturalmente basato sulla "trasparenza" rispetto all'utente del posto dove sono memorizzati ed elaborati i dati.

Il Capo V del GDPR, invece, prevede regole stringenti sul trasferimento di dati presso paesi estranei all'Unione Europea (paese terzo). Questo vuol dire che l'impresa, nello scegliere

il proprio CSP, deve verificare che i dati personali siano collocati in server fisicamente situati in paesi che offrano un livello di protezione adeguato. L'adeguatezza del livello di protezione per un paese terzo è, di norma, stabilito dalla Commissione Europea con una decisione di adeguatezza basata sui seguenti criteri di valutazione:

- caratteristiche dell'ordinamento giuridico con particolare riferimento al riconoscimento dei diritti e delle libertà delle persone;
- effettività della possibilità di difesa in giudizio rispetto al trattamento dei dati personali;
- esistenza di autorità indipendenti di controllo sulla protezione dei dati personali;
- impegni internazionali assunti per la protezione dei dati personali.

È necessario, dunque, che il CSP sia trasparente rispetto alla collocazione dei dati affinché non ci siano spiacevoli sorprese per il cliente con le conseguenti e pesanti sanzioni. D'altra parte, è onere del titolare, cioè dell'impresa, rispettare il principio di *accountability* (tradotto in responsabilizzazione) ovvero riuscire a dimostrare che ha avuto un comportamento diligente (e proattivo) rispetto a questo specifico obbligo.

Il codice di condotta

Il principio di responsabilizzazione e gli altri obblighi del GDPR possono trovare, nel caso del cloud, un valido aiuto nel Codice di Condotta (CoC) per i Fornitori di Servizi Cloud in materia di Protezione dei Dati Personali. L'iniziativa è partita dal Cloud Select Industry Group cioè da un gruppo di CSP leader, riconosciuto dalla Direzione Generale per le Comunicazioni in Rete, i Contenuti e la Tecnologia della Commissione Europea, quando il quadro normativo europeo era basato sulla Direttiva 95/46 successivamente superata dall'entrata il vigore del GDPR. Il percorso, non breve, ha

superato anche il parere richiesto al Gruppo dei Garanti Europei (WP29) del quale sono stati accolti tutti i suggerimenti fino ad arrivare alla versione definitiva che è di maggio 2017 e, quindi, recepisce in pieno le previsioni del nuovo regolamento così come espresse dall'articolo 40.



Il Cloud CoC è un elemento di fiducia di cui l'impresa può avvalersi nella scelta del CSP. Infatti, prima di sedersi al tavolo per la definizione dei dettagli tecnici, il cliente può verificare se il CSP candidato contraente è aderente al CoC e, quindi, procedere con maggiore tranquillità rispetto agli obblighi previsti dal GDPR.

Il CoC, naturalmente, non sostituisce il contratto essendo un codice di comportamento che il CSP si impegna a rispettare nel corso della fornitura. Gli impegni di rilievo previsti dal CoC per i CSP aderenti sono:

- la dislocazione dei dati personali in paesi che offrono le garanzie previste dal Capo V del GDPR;
- l'aggiornamento continuo della lista di collocazioni fisiche dei dati personali e la possibilità di consultazione, in qualsiasi momento, da parte del cliente e delle autorità di controllo;
- la possibilità, per il cliente, di svolgere, in proprio o avvalendosi di un ente terzo, attività di audit finalizzate alla verifica del rispetto del GDPR;
- la restituzione, al termine del contratto, dei dati personali all'azienda cliente secondo i formati concordati e la cancellazione secondo il cronoprogramma previsto in sede di contratto e, comunque, entro un anno dalla fine del rapporto contrattuale.

Infine, un cenno alla governance del CoC è, certamente, un ulteriore elemento di fiducia per i clienti giacché è stato adottato un modello a tre livelli:

1. gestione del framework ovvero governo degli organi e dei flussi consultivi, decisionali ed operativi;
2. gestione dei CSP aderenti ovvero governo delle richieste di adesione da parte dei CSP e del mantenimento dei requisiti previsti;
3. gestione dello stesso CoC ovvero aggiornamento del Codice rispetto alle evoluzioni normative o tecnologiche.

A cura di: **Francesco Maldera**

L’articolo I servizi cloud alla prova del GDPR proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/i-servizi-cloud-alla-prova-del-gdpr/