

Risoluzione sul ricorso all'outsourcing dell'elaborazione dei dati nel cloud

Il software basato sul cloud appare oggi più attraente che mai. Infrastrutture potenzialmente a disposizione di tutti gli utenti Internet (le cosiddette “public cloud”) consentono un’assegnazione dinamica delle capacità di calcolo e di memoria in base alle esigenze dei clienti. Questo effetto di scalabilità è tanto maggiore quanto più estesa – e di norma anche quanto più internazionale – è l’infrastruttura del fornitore cloud (si pensi ai cosiddetti “hyperscaler” come Microsoft, Google o Amazon). Oltre a privati e imprese, anche un numero crescente di enti pubblici ricorre ad applicazioni pronte all’uso fornite direttamente (“Software-as-a-Service”, in breve SaaS) da tali fornitori. Si osserva inoltre che i fornitori cercano sempre più di spingere i loro clienti verso il cloud.

Tuttavia, gli enti pubblici hanno una particolare responsabilità nei confronti dei dati dei propri cittadini. Sebbene possano esternalizzarne il trattamento a terzi, devono garantire che la protezione dei dati e la sicurezza delle informazioni siano rispettate. Prima di esternalizzare dati personali a servizi cloud, le autorità devono quindi analizzare i rischi specifici del caso, indipendentemente dalla sensibilità dei dati, e ridurli a un livello accettabile mediante misure adeguate (cfr. scheda informativa sul cloud di privatim: [l'aide-mémoire cloud de privatim](#)).

Per i seguenti motivi, privatim ritiene nella maggior parte dei casi non ammissibile l'esternalizzazione, da parte di enti pubblici, di dati personali particolarmente degni di protezione o soggetti a un obbligo legale di segretezza verso soluzioni SaaS di grandi fornitori internazionali (come in particolare M365):

1. La maggior parte delle soluzioni SaaS non offre ancora una vera crittografia end-to-end che escluda un accesso del fornitore ai dati in chiaro.
2. Le aziende che operano globalmente offrono un livello di trasparenza insufficiente affinché le autorità svizzere possano verificare il rispetto degli obblighi contrattuali in materia di protezione e sicurezza dei dati. Ciò vale sia per l’implementazione delle misure tecniche e la gestione dei cambiamenti/rilasci (Change-/ Release-Management), sia per l’impiego e il controllo dei collaboratori e dei subappaltatori, che spesso formano lunghe catene di fornitori esterni. A complicare ulteriormente le cose, i fornitori di software possono modificare periodicamente e unilateralmente le condizioni contrattuali.
3. L’utilizzo di applicazioni SaaS comporta pertanto una notevole perdita di controllo. L’ente pubblico non può influire sulla probabilità di una violazione dei diritti fondamentali. Può soltanto attenuare la gravità di eventuali violazioni evitando di trasferire dati particolarmente sensibili al di fuori dell’ambito da esso controllato.
4. Per i dati soggetti a un obbligo legale di segretezza sussiste talvolta una notevole incertezza giuridica circa la possibilità stessa di esternalizzarli a servizi cloud. Non ogni terzo può essere considerato come ausiliario (“Hilfsperson”) solo perché le disposizioni del diritto penale concernenti il segreto d’ufficio o professionale impongono l’obbligo di riservatezza anche agli ausiliari dei detentori del segreto.
5. I fornitori statunitensi possono essere obbligati, in virtù del CLOUD Act emanato nel 2018, a consegnare dati dei propri clienti alle autorità USA senza rispettare le regole dell’assistenza giudiziaria internazionale – anche se tali dati sono conservati in data center situati in Svizzera.

Conclusione: L’utilizzo di soluzioni SaaS internazionali per dati personali particolarmente sensibili o soggetti a un obbligo legale di segretezza da parte di enti pubblici è possibile solo se i dati vengono crittografati direttamente dall’ente responsabile e il fornitore cloud non ha alcun accesso alla chiave.