Cristina Vicarelli
Avvocato

Contrattualistica Cloud: come disciplinare la privacy

Nei servizi cloud è bene prevenire, attraverso contratti e accordi scritti, l'insorgere di problematiche che possono dar luogo a controversie, anche al fine di superare le difficoltà che possono derivare da una a-territorialità che rende complessa l'applicazione di normative tradizionalmente destinate ad operare su base territoriale. Oltre ai parametri tecnici connessi alla continuità del servizio, e alla sua accessibilità e agli aspetti relativi alla sicurezza e alla integrità dei dati, uno degli aspetti più critici è rappresentato dalla tutela dei dati personali, la cui tutela incontra sensibili differenze in ambito europeo ed extraeuropeo.

In assenza di una normativa che armonizzi gli obblighi gravanti sui titolari del trattamento, operare in Europa può comportare l'oggettiva difficoltà di armonizzare le tutele rendendole conformi alle singole normative nazionali, e occorre considerare anche gli adempimenti connessi al trasferimento dei dati in paesi terzi, che potrebbero non conoscere obblighi volti ad apportare adeguata tutela ai dati personali.

Il Gruppo di Lavoro dei Garanti Europei ex art 29 ha provveduto ad individuare gli aspetti più critici che possono inficiare la tutela dei dati personali nei contratti cloud e l'analisi operata si presta ad essere tradotta in un vero e proprio "privacy level agreement" o "PLA" speculare al service level agreement o SLA che, invece, disciplina gli standard tecnici, e che può essere predisposto anche unilateralmente dal fornitore, allo scopo di aumentare la fiducia nei propri servizi.

Soggetti e ruoli privacy

Le prime informazioni da indicare all'interno all'accordo sono sicuramente i dati identificativi del fornitore e soprattutto, ove esistente, del rappresentante nello stato UE, corredati dal ruolo privacy ricoperto, dai recapiti del data Protection Officer e del responsabile della sicurezza dei dati, se previsti in ossequio alle normative applicabili.

Laddove non sia presente il Data Protection Officer è necessario riportare i contatti del soggetto di riferimento al quale gli eventuali interessati possono indirizzare le istanze relative al trattamento dei propri dati personali.

Categorie di dati e modalità di trattamento

E' importante indicare le categorie di dati personali che al cliente è fatto divieto di trattare o comunque conservare in cloud, come ad esempio i dati sensibili relativi allo stato di salute. La ragione di ciò è evidente: le misure di sicurezza non sono sempre le stesse per tutte le tipologie di dati e le leggi nazionali possono vietare di trasferire all'estero dati sensibili o consentirlo solo ove vengano rispettati determinati standard. Chiarire quali tipologie di dati possono essere oggetto dei servizi disciplinati nel contratto di cloud e quali no consente di delimitare il perimetro dei livelli di protezione dei dati sul quale verranno stratificati i successivi livelli di tutela a vantaggio di entrambe le parti.

Detto questo, uno degli aspetti più importanti nell'ambito della contrattualistica in materia di cloud resta la modalità con cui i dati saranno trattati. Nel caso in cui il fornitore sia un mero responsabile del trattamento è essenziale determinare in maniera dettagliata in quali ambiti e con quali modalità il cliente-titolare dei dati potrà fornire le istruzioni necessarie al fornitore- responsabile. Da non trascurare, se possibile, la distinzione tra le attività che verranno eseguite per conto del cliente nell'ambito dell'erogazione del servizio oggetto del contratto principale (vedi la conservazione dei dati) non solo da quelle che saranno effettuate a richiesta del cliente, ma anche da quelle effettuate su iniziativa del solo fornitore, come il back up per citarne una. E, inoltre, sarà bene specificare le modalità attraverso cui il cliente sarà informato di modifiche rilevanti apportate al servizio in cloud. Allo stesso modo, è fondamentale indicare con precisione i luoghi in cui sono ubicati gli strumenti attraverso cui i dati vengono trattati ed, in particolare, i luoghi in cui possono essere praticati la conservazione, la duplicazione il backup e il ripristino dei dati.

Nell'ambito di un accordo un'attenzione particolare dovrà poi essere rivolta all'identificazione dei subfornitori e sub responsabili che partecipano al trattamento dei dati, i limiti posti alla loro eventuale responsabilità e gli accorgimenti utilizzati per assicurare che i requisiti richiesti dal trattamento dei dati personali effettuato siano

soddisfatti (attenzione però perché uno specifico ruolo privacy di "sub responsabile" con nomina conferita direttamente dal responsabile, non è previsto da tutti i Paesi Ue, ad esempio in Italia occorre fare riferimento alla consueta bipartizione titolare – responsabile).

Il successivo step prevede di descrivere le modalità utilizzate per informare il cliente cloud di ogni modifica che riguardi l'aggiunta o la sostituzione di subfornitori o "sub responsabili" -indicazione da prendere con tutte le cautele già evidenziate- prevedendo in ogni momento, in presenza di simili modifiche, la possibilità per il cliente di recedere dal contratto.

E' evidente che in questi casi occorrerà distinguere gli aspetti che possono essere considerati alla stregua di "metriche del servizio" seppure relative al trattamento dei dati personali, e quelli che invece necessiteranno di una vera e propria contrattualizzazione, in modo da ripartire congruamente diritti e obblighi nel contratto principale e nel PLA, dato che non sempre sarà possibile rinvenire la radice di tali obblighi nella normativa applicabile alle parti.

Il trasferimento dei dati all'estero

Altra spinosa questione riguarda il trasferimento dati. Per scongiurare il rischio di violare la normativa privacy e per tutelarsi da eventuali sanzioni è essenziale indicare quando i dati possono essere trasferiti, duplicati (backup) e/o ripristinati in paesi terzi, senza dimenticare di specificare se questo rientra nel normale modus operandi o se si tratta di una **procedura di emergenza**. Se la legge applicabile impone limiti e restrizioni al trasferimento dei dati oltre i confini nazionali è opportuno individuare la base giuridica che renda possibile il trasferimento, senza dimenticare di indicare se i dati saranno trasferiti oltre i confini dell'Unione Europea. Nel caso in cui si preveda il trasferimento oltre i confini dell'Unione Europea è necessario identificare la base giuridica e verificare la presenza di particolari normative in vigore, come ad esempio safe harbor, clausole tipo o decisioni di adeguatezza.

Misure di sicurezza

Sul fronte delle misure di sicurezza è bene indicare specificamente le misure tecniche, fisiche ed organizzative che saranno poste in essere per proteggere i dati personali da sottrazione o distruzione intenzionale o accidentale, perdita accidentale, alterazioni, uso non autorizzato, modifiche, divulgazione, diffusione, accessi non previsti e ogni altra forma di trattamento illecito. Oltre a garantire il rispetto delle misure di sicurezza definite "minime" dal legislatore e direttamente rinvenibili nella normativa tecnica, occorrerà individuare le misure idonee descrivendo le misure fisiche tecniche ed organizzative volte ad assicurare disponibilità dei dati, integrità, riservatezza, trasparenza, segregazione dei rischi, finalità del trattamento, possibilità di intervento, portabilità ed accountability.

In quest'ultimi due casi, in particolar modo, due sono le rispettive questioni da tenere bene a mente:

- Denotare i **formati dei dati**, oltre alle relazioni logiche ed i costi associati alla loro portabilità, le applicazioni ed i servizi e, al tempo stesso, fissare per iscritto come e a quale **costo** il fornitore assisterà il cliente in una eventuale migrazione verso un altro provider o per tornare a un trattamento presso i propri sistemi potrebbe rivelarsi essenziale in caso di necessità;
- Descrivere di quali policy o procedure o modelli il fornitore si sia dotato per garantire e **dimostrare la conformità alla normativa vigente**, anche attraverso regolamenti interni o altri accorgimenti che dimostrino la necessaria compliance, ad esempio documentando tutte le operazioni di trattamento svolte sotto la sua responsabilità, prevedendo efficaci controlli e sistemi integrali di registrazione degli accessi potrebbe mettere al riparo da grattacapi di non poco valore.

Verifiche e controlli

Occorre non dimenticare che il Titolare ha uno specifico onere di controllo sull'operato del responsabile. Anche le modalità attraverso le quali questi controlli vengano consentiti, e le possibilità di delegarle a soggetti terzi dovranno essere declinate nell'accordo (ed, eventualmente, come sempre, pattuite contrattualmente). In particolare occorrerà:

- Indicare se il cliente abbia la facoltà – o il diritto o la potestà- di fare verifiche dirette o disporre forme di audit per accertarsi che le misure inerenti la riservatezza e la sicurezza definite nel piano siano effettivamente adottate. Descrivere

dettagliatamente le condizioni e le forme di verifica (report, audit o altro), specificando il tipo di controllo che potrà esercitare il cliente, come la accessibilità ai report di log, o l´auditing circa i trattamenti più rilevanti operati dal fornitore o dai subfornitori.

- Delegare a terzi, scelti nell'accordo delle parti, l'attività di controllo oppure indicare, se sono già previsti, quali report delle verifiche effettuate da terzi certificatori indipendenti verranno forniti al cliente, il loro ambito, la loro frequenza e quali di essi vengono periodicamente aggiornati, e se verrà fornito un report completo o solo uno schema di sintesi.
- Indicare le procedure di conservazione adottate dal fornitore e le condizioni per la restituzione o la distruzione dei dati personali una volta che il servizio principale abbia avuto termine. Queste comprendono le regole di conservazione dei dati, la cancellazione, la conservazione dei dati per adempiere ad obblighi di legge.
- Definire in che misura il fornitore coopererà con il cliente, in modo da assicurare l´adempimento della normativa dettata in tema di protezione dei dati personali, ad esempio consentendo al cliente di garantire agli interessati un effettivo esercizio dei loro diritti.
- Descrivere le procedure adottate per gestire e soddisfare le richieste di informazioni da parte di Autorità di contrasto alla criminalità, con particolare attenzione alle procedure di comunicazione ai clienti coinvolti, quando ciò non sia vietato

Scioglimento anticipato del contratto e altre cautele

Per mettersi al riparo dalle controversie è utile precisare quali garanzie sono offerte al cliente nel caso in cui il fornitore o i suoi subfornitori recedano o comunque pongano fine al rapporto contrattuale o si rendano inadempienti agli obblighi assunti con il PLA, e quali rimedi **contrattuali** siano previsti (comprese manleve o penali o ristori anche dei danni eventualmente causati a terzi interessati) per gli inadempimenti in ordine a sicurezza, sistema di verifiche, comunicazione delle violazioni dei dati personali, portabilità e / o obblighi di conservazione.

Nell'ottica di un offrire un servizio più appetibile è buona regola descrivere eventuali polizze che coprano i servizi offerti dal fornitore e da questi stipulate, se esistenti, dettagliandone l´ambito di applicazione e l´eventuale inclusione di fattispecie relative alla violazione di dati personali, così come indicare i recapiti che il fornitore destina al ricevimento dei reclami o a richieste di chiarimenti in ordine al trattamento effettuato. Segnalare eventuali terzi ai quali deferire la risoluzione delle controversie insorte, se la normativa lo consente, ad esempio autorità indipendenti, arbitri o servizi di mediazione o conciliazione.

L'elencazione degli aspetti critici operata dal Gruppo di Lavoro dei Garanti Europei ex art 29 offre una prospettiva ampia ed esaustiva delle problematiche che possono emergere in ordine alla gestione dei dati personali nei servizi cloud. Nella pratica, tuttavia, occorrerà distinguere attentamente gli aspetti che dovranno essere oggetto di clausole contrattuali e quelli che potranno, invece, essere inseriti direttamente nel PLA (che correda il testo pattizio senza sostituirlo), facendo particolare attenzione ad eventuali conflitti con le norme imperative che incidono sul contratto principale, in modo da evitare di appesantire il contratto cloud con documentazioni copiose e elenchi sterili di impegni i cui inadempimenti non potrebbero essere azionati.