privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

Promemoria

CLOUD COMPUTING

1 Introduzione

Questo promemoria è rivolto agli organi pubblici dei Cantoni e dei Comuni che stanno valutando l'impiego, o che già impiegano, i servizi Cloud (Cloud-Services).

L'impiego di servizi Cloud costituisce un'elaborazione su mandato (detta anche esternalizzazione o Outsourcing) e deve perciò ottemperare alle stesse esigenze valide per l'elaborazione di informazioni nell'ambito dell'Outsourcing tradizionale di un'elaborazione di informazioni. Poiché, paragonato all'Outsourcing tradizionale, l'impiego di servizi Cloud implica un rischio nettamente superiore di violazione delle condizioni quadro e, in caso di elaborazione di dati personali, dei diritti della personalità, va prestata particolare attenzione alle singole condizioni poste dalle leggi sulla protezione dei dati (e della trasparenza).

Il punto di partenza per l'impiego di servizi Cloud è un'analisi dei rischi che definisca in modo preciso e puntuale le condizioni cui vanno assoggettati i fornitori di servizi Cloud così come il contenuto del contratto da concludere con questi ultimi in forma scritta. Le specificità del Cloud devono essere regolamentate nel dettaglio e l'attuazione delle misure concordate va controllata regolarmente.

2 Cloud Computing e Outsourcing

L'impiego di servizi Cloud costituisce, dal punto di vista del diritto della protezione dei dati (e della trasparenza), un'elaborazione su mandato. Chi ne fa uso deve perciò attenersi alle relative condizioni stabilite nelle leggi sulla protezione dei dati (e sull'informazione). Gli organi pubblici possono far capo ai servizi Cloud se sono in grado di assumere i loro obblighi in materia di protezione dei dati e di sicurezza delle informazioni. In questo senso, gli organi pubblici sono (e rimangono anche dopo l'attribuzione del mandato a terzi) responsabili dell'elaborazione dei dati.

Le peculiarità del Cloud e i rischi che ne conseguono, come ad esempio l'impiego di un'infrastruttura da parte di più utenti, vanno fronteggiati con adeguate misure di compensazione dei rischi. Vanno perciò presi in considerazione ulteriori elementi sia nella scelta del fornitore Cloud e delle offerte di servizi Cloud, sia nella stesura del contratto come

privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati
c/o Datenschutzbeauftragter des Kantons Zürich
Postfach, CH-8090 Zürich
Tel. +41 (43) 259 39 99, Fax +41 (43) 259 51 38
geschaeftsstelle@privatim.ch, www.privatim.ch

pure nell'implementazione delle misure di compensazione dei rischi. Le sfide maggiori si pongono a livello della trasparenza, dei controlli e, più generalmente, dell'assunzione della responsabilità da parte dell'organo pubblico.

3 Analisi dei rischi e scelta del fornitore

Per i loro sistemi e le loro applicazioni informatiche, gli organi pubblici eseguono un'analisi dei rischi. A dipendenza del contenuto dell'elaborazione di dati in questione vanno, da un lato, definiti gli obiettivi di protezione (con riferimento alla confidenzialità, disponibilità e integrità, eventualmente anche della responsabilità e della verificabilità) e, dall'altro, individuato il potenziale di pericolo. Da queste valutazioni emergono gli elementi per la scelta del fornitore e per l'offerta Cloud: in effetti esse definiscono le esigenze di base che il fornitore deve rispettare dal profilo organizzativo, tecnico e giuridico.

I rischi specifici del Cloud vanno analizzati in particolare per quanto riguarda i seguenti aspetti:

- assunzione delle responsabilità delle due parti contraenti;
- perdita del controllo o impossibilità di esercitare gli obblighi di controllo;
- attuabilità dei diritti di cancellazione e di rettifica;
- garanzia di un livello di protezione dei dati equivalente;
- realizzazione delle necessarie misure di sicurezza nel settore delle tecnologie dell'informazione e della comunicazione;
- verificabilità dei decorsi e dei processi;
- ricostruibilità delle elaborazioni di dati;
- perdita di dati;
- abuso di dati;
- restrizione della disponibilità dei servizi;
- portabilità e interoperabilità.

Il fornitore Cloud deve informare sulle condizioni quadro legali, tecniche e organizzative del servizio offerto. Strumenti di ausilio in questo senso possono essere i certificati o i rapporti audit indipendenti, nella misura in cui rendono trasparenti determinati aspetti del servizio. La loro autorevolezza e la loro validità dipendono dal rispetto di standard nazionali e internazionali.

4 Forma e contenuto del contratto

L'organo pubblico deve poter assumere anche nella struttura Cloud la propria responsabilità, dedotta dal diritto della protezione dei dati (e della trasparenza). Va perciò definito in

forma scritta e in modo dettagliato, in un contratto, chi è responsabile ai sensi della normativa sulla protezione dei dati (e della trasparenza) e per che cosa. Se, per elaborare dati personali, in particolare dati meritevoli di particolare protezione e profili della personalità, si opta per una soluzione Cloud, non è di regola sufficiente accettare le condizioni generali di contratto (CGC) standard di un fornitore generico.

4.1 Controllo

Le prerogative di controllo dell'organo pubblico e delle autorità di sorveglianza indipendenti (incaricato della protezione dei dati, controllo delle finanze) devono essere previste a livello contrattuale, con particolare attenzione alla possibilità di effettuare controlli sul posto.

Inoltre, il fornitore Cloud deve obbligarsi a far eseguire regolarmente controlli esterni secondo gli standard internazionali di audit e a mettere a disposizione dell'organo pubblico i risultati degli esami effettuati dagli organismi di controllo indipendenti.

4.2 Diritti delle persone interessate

Il fornitore Cloud deve garantire contrattualmente il diritto di accesso delle persone interessate ai loro dati personali registrati, nonché il diritto di rettifica e di cancellazione.

4.3 Luogo dell'elaborazione dei dati

In ogni caso, il fornitore Cloud deve impegnarsi in forma scritta a informare su tutti i possibili luoghi in cui i dati sono elaborati. Cambiamenti di luogo devono essere annunciati e l'organo pubblico deve autorizzarli.

In caso di elaborazione di dati sensibili (dati personali meritevoli di particolare protezione o profili della personalità, oltre che dati che soggiacciono a particolari norme di segretezza o che, per motivi estranei alla protezione dei dati, vanno considerati sensibili) occorre garantire che le autorità straniere non possano accedervi fisicamente (ad esempio sequestrandoli). In questi casi, è necessario garantire contrattualmente che tutte le elaborazioni di dati avvengano esclusivamente in Svizzera.

4.4 Livello di protezione dei dati equivalente

Le trasmissioni di dati all'estero soggiacciono a specifiche disposizioni di protezione dei dati (e della trasparenza). Lo stesso vale anche per l'uso di servizi Cloud, poiché l'organo pubblico rimane responsabile dell'elaborazione. Se i servizi Cloud comportano l'elaborazione di dati personali, un'esternalizzazione del trattamento all'estero è possibile unicamente nel caso in cui esista una protezione dei dati equivalente a quella svizzera e/o vengano implementate misure di sicurezza supplementari.

4.5 Rapporti di subappalto

Rapporti di subappalto devono essere noti prima della conclusione del contratto. Accordi successivi di subappalto possono essere sottoscritti solo se l'organo pubblico ne sia informato e li abbia autorizzati. I subappaltatori devono impegnarsi a rispettare le direttive del fornitore Cloud. Inoltre, in caso di elaborazione di dati sensibili, i subappaltatori soggiacciono alle stesse condizioni del fornitore Cloud per quanto riguarda la sede dell'azienda e il luogo di elaborazione dei dati.

4.6 Diritto applicabile, attuazione del diritto

La questione di sapere se il diritto svizzero, in particolare quello della protezione dei dati (e della trasparenza), sia applicabile, dipende dalla regolamentazione concreta. È comunque determinante che l'organo pubblico, il quale rimane responsabile, possa giuridicamente ed effettivamente assumere la sua responsabilità. Esclusioni della responsabilità contenute nelle CGC del fornitore Cloud, così come il foro giudiziario o la sede all'estero del fornitore Cloud, possono costituire un impedimento. Non basta convenire unicamente il foro in Svizzera; in caso di elaborazione di dati sensibili occorre prestare attenzione a che la sede del fornitore Cloud (così come il luogo dell'elaborazione dei dati: cifra 4.3) sia in Svizzera. Caso contrario, l'organo pubblico potrebbe vedersi eventualmente costretto a ottenere una sentenza giudiziaria all'estero o a far imporre una sentenza giudiziaria svizzera all'estero. Ciò potrebbe rappresentare una sfida eccessiva per l'organo pubblico, e metterebbe di conseguenza in dubbio l'attuazione del diritto e l'assunzione delle proprie responsabilità.

4.7 Misure di sicurezza tecniche e organizzative

Confidenzialità, integrità, disponibilità, autenticità e ricostruibilità devono essere garantite anche in caso di uso di servizi Cloud. Le categorie di dati da elaborare e i bisogni di sicurezza vanno previsti contrattualmente. Occorre prevedere l'obbligo del fornitore Cloud di informare regolarmente l'organo pubblico sull'attuazione delle principali misure di sicurezza nel settore delle tecnologie dell'informazione e della comunicazione. Inoltre, il fornitore Cloud deve impegnarsi a informare l'organo pubblico su eventi rilevanti per la sicurezza.

Il fornitore Cloud deve garantire gli obiettivi di sicurezza previsti, anche se di regola in modo non esaustivo, dalle disposizioni sulla sicurezza delle informazioni contenute nelle normative sulla protezione dei dati (e sull'informazione). Egli deve prevedere in un concetto di sicurezza delle informazioni le misure tecniche e organizzative come la procedura crittografica, l'Identity e Access Management, la gestione delle urgenze, ecc. In caso di elaborazione di dati sensibili (dati meritevoli di particolare protezione e profili della personalità), il fornitore Cloud deve gestire le misure tecniche e organizzative in un sistema di gestione per la sicurezza delle informazioni.

Devono poi essere concordate in modo specifico le misure tecniche e organizzative che garantiscono la portabilità, l'interoperabilità e la separazione logica dei dati.

5 Attuazione delle misure

L'attuazione delle condizioni quadro tecniche, organizzative e giuridiche, come previste nel contratto, deve essere regolarmente controllata dall'organo pubblico.

6 Bibliografia e fonti d'informazione utili

- Organo direzionale informatica della Confederazione (ODI) del Dipartimento federale delle finanze, Cloud Computing, la strategia delle autorità svizzere 2012-2020

- Incaricato federale della protezione dei dati e della trasparenza IFPDT, Spiegazioni sul Cloud Computing, ottobre 2011

- Gruppo di lavoro articolo 29 per la protezione dei dati dell'Unione europea, Parere 05/12 sul cloud computing, 1° luglio 2012

- Garante europeo della protezione dei dati, L'informatique en nuage (domande e risposte)

- Garante per la protezione dei dati personali della Repubblica italiana, Cloud computing: indicazioni per l'utilizzo consapevole dei servizi, Schede di documentazione, settembre 2011;

- Gruppi di lavoro Tecnica e Media della Conferenza degli incaricati della protezione dei dati della Repubblica federale di Germania e dei Länder, Orientierungshilfe Cloud Computing, versione 1.0, 26 settembre 2011;

- Risoluzione dell'82a Conferenza degli incaricati della protezione dei dati della Repubblica federale di Germania e dei Länder, Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing, 28/29 settembre 2011, Monaco di Baviera;

- Agenzia europea della sicurezza della rete e dell'informazione ENISA, Cloud Computing, benefits, risks and recommendations for information security, novembre 2009;

- Bundesamt für Sicherheit in der Informationstechnik (Germania), Sicherheitsempfehlungen für Cloud Computing Anbieter, Mindestsicherheitsanforderungen in der Informationssicherheit, 2011

- Bundesamt für Sicherheit in der Informationstechnik (Germania), Spezifische Massnahmen zur Trennung der Datenbeständen, Gefährdungen und Gegenmassnahmen beim Einsatz von VCE Vblock, versione 2.5, 22 dicembre 2011

- Philipp Mittelberger/Gabriele Binder, Datenschutzrechtliche Chancen und Risiken von Cloud Computing, Jus & News 2011/2, pag. 163 segg.;

- Uwe Heck/Willy Müller, Vorstudie zu Cloud Computing in Schweizer Behörden, versione 1.0, 21 ottobre 2010