School of Management

POLITECNICO DI MILANO

DIPARTIMENTO DI INGEGNERIA GESTIONALE

MIP

OSSERVATORI.NET digital innovation

www.osservatori.net

Aspetti legali e contrattuali del cloud computing

Annamaria Italiano

21 Marzo 2015

OSSERVATORI.NET digital innovation

Agenda

Cos'è il cloud computing

- Definizione
- Caratteristiche essenziali
- Modelli di servizio e di deployment

Il cloud dal punto di vista contrattuale

- Rigidità degli accordi
- Le clausole contrattuali "unfair" più comuni nella prassi

Cloud computing e protezione dei dati personali

- I principali rischi connessi all'adozione di tecnologie cloud
- Il quadro normativo
- Ripartizione delle responsabilità tra i soggetti del rapporto contrattuale (indicazioni del Garante Privacy e Opinion n. 5/2012 art. 29 WP)
- Il trasferimento dati al di fuori dell'UE
- La scelta di un cloud provider di qualità (il "decalogo" del Garante Privacy e le certificazioni indipendenti)

Cos'è il cloud computing

La definizione di cloud computing data dal National Institute Standards and Technology

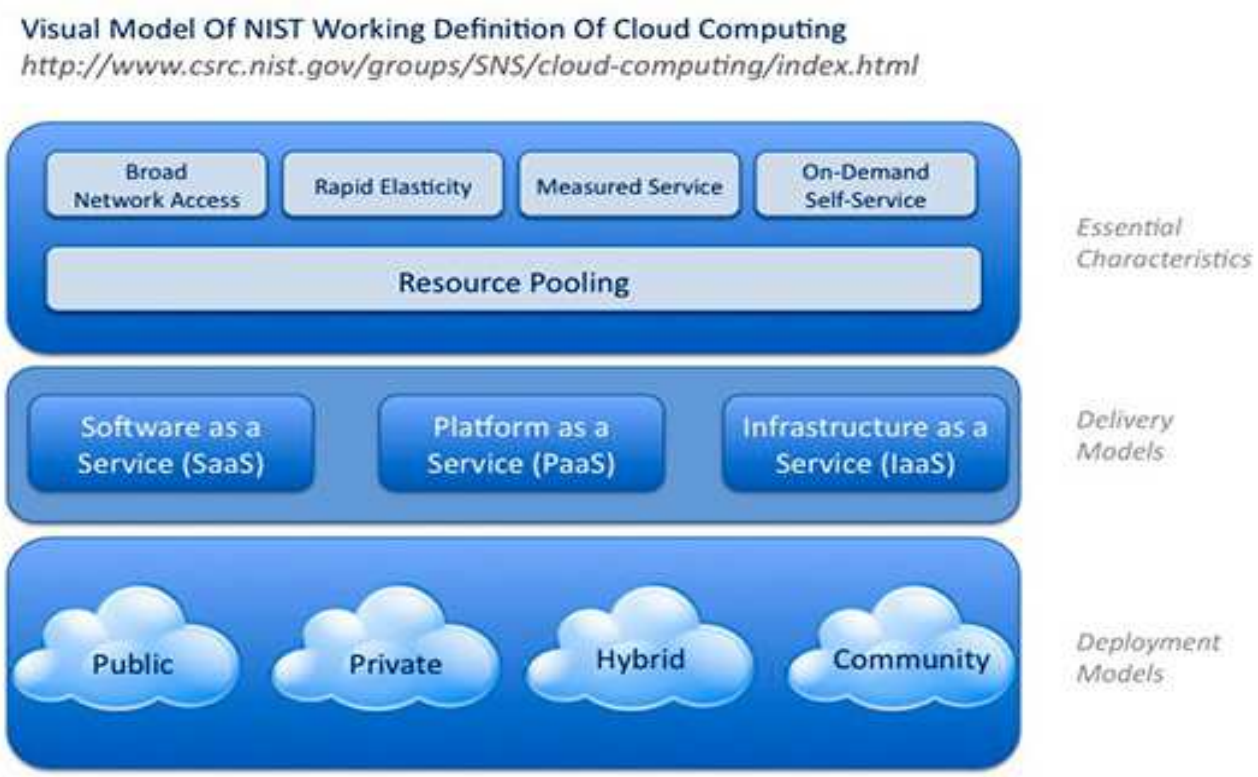
"Cloud computing is a model for enabling ubiquitous, convenient, **on-demand network access** to a **shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released **with minimal management effort** or service provider interaction. This cloud model is composed of **five essential characteristics, three service models, and four deployment models**".

"Il cloud computing è un modello per abilitare, **tramite la rete**, l'accesso diffuso, agevole e **a richiesta**, ad un **insieme condiviso e configurabile di risorse** di elaborazione (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con **minimo sforzo di gestione** o di interazione con il fornitore di servizi. Questo modello cloud è composto di **cinque caratteristiche essenziali, tre modalità di servizio e quattro modelli di distribuzione**".

I vantaggi del cloud computing

- **Accesso in mobilità** (la connessione ai dati può avvenire da qualsiasi posto e in qualsiasi momento)
- **Indipendenza dalle periferiche** (grazie alla fruizione dei servizi online, non si è vincolati ad utilizzare particolari hardware o determinate configurazioni di reti)
- **Riduzione dei costi** (acquisto, configurazione, installazione, manutenzione e dismissione di hardware e software)
- **Flessibilità e scalabilità** (è possibile agevolmente espandere o contrarre l'infrastruttura utilizzata sulla base delle contingenti o mutate esigenze aziendali)
- **Maggiore sicurezza per la protezione dei dati**.

Cos'è il cloud computing



Caratteristiche essenziali dei servizi cloud

- **On demand self-service** (completa autonomia del cloud consumer dell'approvvigionamento delle risorse)
- **Broad network access** (funzionalità accessibili attraverso la rete, attraverso meccanismi standard)
- **Resource pooling** (modello di fruizione multi-tenant)
- **Rapid elasticity** (rapidità ed elasticità di allocazione e rilascio)
- **Measured Service** (controllo ed ottimizzazione delle risorse, monitoraggio delle prestazioni e dei livelli di carico)

Modelli di servizio del cloud computing		
Software as a Service (Saas)	**Platform as a Service (Paas)**	**Infrastructure as a Service (Iaas)**
Applicazione software che può essere utilizzata su richiesta. Il fornitore del servizio installa l'applicazione nei propri data center e fornisce agli utenti un'interfaccia per utilizzarla	Il fornitore mette a disposizione la propria piattaforma e offre soluzioni per lo sviluppo e l'hosting evoluto di applicazioni	Infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale è possibile installare ed eseguire il software necessario all'utente

Modelli di fruizione del cloud computing			
Private cloud	**Public cloud**	**Community cloud**	**Hybrid cloud**

Il cloud e il settore dell'istruzione

- Applicazioni che facilitano l'organizzazione/amministrazione
- Applicazioni che facilitano l'amministrazione con profili connessi allo svolgimento dell'attività scolastica (es. registro online)
- Applicazioni che integrano l'offerta didattica
- Applicazioni che consentono lo storage di grandi volumi documentali

Il Cloud computing dal punto di vista legale

Mancanza di un quadro normativo organico e specifico

Potenziali rischi di compliance normativa (con particolare riferimento alla materia della protezione dei dati)

Il ricorso a forme di esternalizzazione non può essere inteso come «deresponsabilizzazione»

Marcata standardizzazione delle clausole contrattuali

- Esigenza dei cloud service provider di disciplinare e gestire in maniera uniforme una molteplicità di rapporti negoziali.
- Scarso o nullo potere negoziale degli utenti finali.

Mancanza di una specifica disciplina di legge

- Contratto atipico con causa mista.
- In mancanza di puntuale dettato contrattuale, difficoltà di inquadramento dei contratti in questione secondo le tradizionali classificazioni giuridiche (es. distinzione tra obbligazioni di mezzi ed obbligazioni di risultato.

Rigidità degli accordi , asimmetria negoziale e unfairness delle clausole

Esclusione di garanzie

I servizi cloud sono forniti «nelle condizioni in cui si trovano» e «per quanto disponibili». In particolare, non si garantisce che i servizi offerti:

- funzionino senza interruzioni, tempestivamente, siano sicuri o privi di errori, né che eventuali errori vengano tempestivamente corretti;
- siano conformi alle specifiche esigenze dell'utente;
- non violino i diritti dei terzi (qualsiasi materiale scaricato o ottenuto dai servizi cloud, viene scaricato od ottenuto a completa discrezione ed esclusivo rischio dell'utente).

Le clausole contrattuali «critiche»

Limitazione/esclusione di responsabilità

- Escludono o limitano ad una soglia massima di danno risarcibile la responsabilità del cloud provider per danni di qualsiasi genere o natura.

- Giustificabili in ragione delle caratteristiche di multi-utenza dei contratti in questione, ma eccessivamente sbilanciate in favore del cloud provider quando ne limitino la responsabilità per danni conseguenti ad eventi che egli avrebbe l'obbligo di prevedere e gestire (es. limitazione di responsabilità in caso di perdita di dati di titolarità dell'utente).

Le clausole contrattuali «critiche»

Attenzione anche alle clausole che stabiliscono:

- Livelli di servizio
- Limitazione di responsabilità per “forza maggiore”
- Limitazione di responsabilità per “fatto del terzo”
- Decadenze dal diritto di contestare i corrispettivi e/o il servizio
- Legge applicabile e foro competente

Le clausole contrattuali «critiche»

Diritto di modifica unilaterale

- Può riguardare alternativamente o cumulativamente le condizioni tecniche e contrattuali, i livelli di servizio o i corrispettivi contrattualmente pattuiti.

- Le modifiche possono essere portate a conoscenza dell'utente tanto attraverso comunicazioni dirette, quanto attraverso mera pubblicazione sul sito web del cloud provider, imponendosi in tal modo all'utente un «onere informativo» ed un meccanismo di accettazione tacita delle condizioni modificate.

- Diritto di recesso dal contratto quale unico rimedio accordato all'utente dissenziente.

Le clausole contrattuali «critiche»

Diritto di sospensione del servizio (temporaneo o definitivo)

Viene generalmente previsto in una o più delle seguenti ipotesi:

- ritardo (più o meno consistente) nel pagamento di uno o più canoni di servizio;
- inadempimento da parte dell'utente di una qualsiasi delle obbligazioni contrattualmente assunte;
- in ogni momento e per qualsiasi ragione, ad esclusiva discrezione del cloud provider.

I principali rischi connessi all'adozione dei servizi di cloud computing

- Perdita del controllo diretto ed esclusivo sui dati di propria titolarità.
- Spesso il servizio prescelto viene fornito attraverso le prestazioni di subfornitori diversi da quelli con cui l'utente stipula il contratto.
- La disponibilità dei dati allocati nella nuvola non è incondizionatamente garantita.
- L'utente non sempre è messo in grado di conoscere l'ubicazione dei data center.
- Rischio di vendor lock-in.
- Rischi per la confidenzialità e la riservatezza dei dati.

Cloud e protezione dei dati personali

Fonti normative

- Codice Privacy italiano (d. lgs. 196/2003)
- Direttiva 95/46/CE sul trattamento e la protezione dei dati personali
- Direttiva e-privacy 2002/58/CE (modificata dalla direttiva 2009/136/CE), che si applica al trattamento dei dati personali nel settore delle comunicazioni elettroniche
- Nuovo Regolamento UE in materia di dati personali (in corso di approvazione)

Spunti di interesse provenienti da studi in ambito privacy

- Gruppo di lavoro ex art. 29, Parere 05/2012 - Cloud Computing
- La mini guida del Garante del giugno 2012 : “Proteggere i dati per non cadere dalle nuvole”
- Il vademecum del Garante: «La Privacy tra i banche i scuola» (2010)
- Commission expert group

Il concetto di dato personale

Articolo 4 Codice Privacy

Per «**dato personale**» si intende qualsiasi informazione associabile a una persona fisica, identificata o identificabile, a condizione che:

- il riferimento riguardi una **persona fisica** (dunque non una persona giuridica, un ente, una p.a., ecc.)

- Esista un **elemento connettivo**, anche indiretto, tra informazione e persona fisica (anche in presenza di **relazioni multiple**)

Il concetto di dato personale

Si considerano «**dati sensibili**» quelli idonei a rivelare

- L'origine razziale ed etnica
- Le convinzioni religiose, filosofiche o di altro genere
- Le opinioni politiche
- L'adesione a partiti, associazioni od organizzazioni a carattere religioso, filosofico, politico
- Lo stato di salute
- La vita sessuale

Si considerano «**dati giudiziari**» quelli idonei a rivelare:

- I provvedimenti di cui all'art. 3, comma 1, lett. da a) a o) e da r) a u) del d.p.r. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti
- La qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.

Il trattamento dei dati sensibili in ambito scolastico

- Può assumere rilievo nella fase amministrativa e gestionale della struttura scolastica

- Va considerato puramente eventuale nel corso dell'attività propriamente didattica

Il Garante ha precisato che

- «*L'assegnazione da parte degli insegnanti di temi in classe, anche se attinenti alla sfera personale o familiare degli alunni, è del tutto lecita e rispondente alle* ***funzioni attribuite all'istituzione scolastica***»
- «*Restano peraltro fermi gli obblighi di riservatezza già previsti per il corpo docente, a livello di* ***segreto d'ufficio e professionale****, nonché, quelli relativi alla* ***conservazione*** *dei dati personali eventualmente contenuti nei temi predisposti dagli alunni»*

Ripartizione di ruoli e responsabilità tra i diversi attori

Art. 4 Codice Privacy

Titolare

«La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza».

Responsabile

«La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali».

Interessato

«la persona fisica cui si riferiscono i dati personali».

Le indicazioni del Garante sul riparto degli obblighi tra e parti del trattamento

Il titolare e il responsabile del trattamento.

- **La pubblica amministrazione o l'azienda, "titolare del trattamento" dei dati personali, che trasferisce del tutto o in parte il trattamento di dati personali a un fornitore, deve procedere a designare il fornitore dei servizi cloud "responsabile del trattamento"**

- **In caso di violazioni commesse dal fornitore** (o da un subfornitore), **anche il titolare sarà chiamato a rispondere dell'eventuale illecito**. Non sarà sufficiente per giustificare una eventuale violazione affermare di non avere avuto possibilità di negoziare clausole contrattuali o modalità di controllo stringenti: **il cliente di servizi cloud può sempre rivolgersi ad altri fornitori che offrono maggiori garanzie, in particolare per il rispetto della normativa sulla protezione dei dati**

- Il Codice della privacy prevede tra l'altro, che **il titolare eserciti un potere di controllo nei confronti del responsabile del trattamento**, verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati

Le indicazioni del Garante sul riparto degli obblighi tra le parti del trattamento

Trasferimento dei dati fuori dell'Unione Europea.

- Il Codice della privacy definisce regole precise per il trasferimento dei dati personali fuori dall'Unione europea e vieta, in linea di principio, il trasferimento "anche temporaneo" di dati personali verso uno Stato extraeuropeo, qualora l'ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela
- **Il titolare del trattamento dovrà quindi tenere in debito conto anche il luogo dove vengono conservati i dati e quali sono i trattamenti previsti all'estero**

Sicurezza dei dati.

- Il titolare del trattamento deve assicurarsi che siano adottate misure tecniche e organizzative volte a ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole
- **Occorre quindi contrattualmente imporre ai fornitori non solo il rispetto delle misure minime di sicurezza previste dall'allegato B al d.lgs 196/03 ma anche un livello di sicurezza che, di volta in volta in considerazione delle caratteristiche di ogni contratto, possa essere ritenuto idoneo**

I diritti dell'interessato.

- I soggetti pubblici e le imprese che decidono di avvalersi di servizi cloud per gestire i dati personali dei loro utenti o clienti non devono dimenticare che il Codice della privacy attribuisce agli interessati (le persone a cui si riferiscono i dati) precisi diritti

I contenuti dell'opinion 5/2012 Art. 29 WP

Obblighi di protezione dei dati nella relazione cliente/fornitore

- **Trasparenza**

Deve informare tanto il rapporto tra cliente cloud ed eventuali interessati – che per legge hanno diritto a conoscere l'identità del titolare, le finalità del trattamento e i destinatario o le categorie di destinatari dei dati, che possono comprendere incaricati e subincaricati del trattamento medesimo – tanto il rapporto tra cliente cloud, cloud provider ed eventuali ulteriori subcontraenti. Sotto tale ultimo profilo, il provider sarà tenuto a fornire **un'informativa dettagliata e completa** che comprenda, tra le altre cose, **l'elenco dei responsabili e dei sub-responsabili**, **l'indicazione dei luoghi in cui i dati risiedono** o possono essere trattati, nonché precise informazioni circa la comunicazione dei dati a terzi e il trasferimento dei dati in paesi fuori dall'Unione Europea.

- **Specificazione e limitazione delle finalità del trattamento**

I dati personali dovranno essere raccolti per **finalità determinate**, **esplicite e legittime** e successivamente trattati in modo non incompatibile e non eccedente rispetto a tali finalità**.**

I contenuti dell'opinion 5/2012 Art. 29 WP

Obblighi di protezione dei dati nella relazione cliente/fornitore

- **Conservazione e cancellazione dei dati**

I dati personali dovranno essere conservati in modo da consentire l'identificazione degli interessati per un arco temporale non superiore a quello strettamente necessario al conseguimento delle finalità per le quali sono rilevati o successivamente trattati. I dati personali non più necessari dovranno essere cancellati o resi anonimi. Ove la cancellazione non sia possibile stante l'esistenza di precise norme di legge che impongono la conservazione (es. normative fiscali), l'accesso a tali dati dovrà essere bloccato.

- **Tutele contrattuali nel rapporto tra Titolare e Responsabile del trattamento**

In generale: il titolare del trattamento ha l'onere di scegliere un responsabile che presenti sufficienti garanzie in termini di misure tecniche ed organizzative per la protezione e la sicurezza dei dati. Il contratto dovrà essere stipulato per iscritto e dovrà sancire in particolare l'obbligo per il responsabile di seguire le istruzioni impartite dal titolare del trattamento.
In particolare: l'opinion 5/2012 prevede una serie di contenuti contrattuali specifici che dovranno essere disciplinati al minimo negli accordi tra clienti e cloud provider.

IL CONTENUTO DEI CONTRATTI

1. **Livelli di servizio** (SLA) espressi in termini **oggettivi e misurabili** e le **sanzioni correlate** al loro mancato rispetto
2. Specificazione delle **misure di sicurezza** che il fornitore cloud è tenuto a rispettare, a seconda della natura dei dati da proteggere e dei rischi del trattamento
3. **Oggetto ed orizzonte temporale** del servizio cloud da fornire
4. **Portata, modalità e finalità del trattamento dati** effettuato dal fornitore
5. Specificazione delle modalità di **restituzione** o **cancellazione dei dati** alla cessazione del rapporto
6. Previsione di una **clausola di riservatezza** vincolante per il fornitore e per i suoi dipendenti specificamente autorizzati all'accesso ai dati
7. Obbligo del fornitore di sostenere il cliente nell'agevolare l'esercizio, da parte degli interessati, dei loro **diritti di accesso ai dati, rettificazione o cancellazione**

IL CONTENUTO DEI CONTRATTI

8. Obbligo del fornitore di **indicare tutti i subcontraenti autorizzati**, nonché di informare il cliente in merito ad eventuali cambiamenti degli stessi, ai quali il cliente avrà diritto di **opporsi** o di **risolvere il contratto**

9. Obbligo del fornitore di garantire che **gli accordi con i subfornitori rispecchino le disposizioni dell'accordo stipulato con il cliente**

10. Obbligo del fornitore di **comunicare al cliente eventuali violazioni** che possano costituire un rischio per i suoi dati

11. Obbligo del fornitore di **fornire un elenco dei luoghi dove saranno trattati i dati**

12. Espresso diritto del titolare di **controllare l'operato del responsabile**, a fronte del dovere di quest'ultimo di collaborare

13. Obbligo del fornitore di **informare il cliente in merito a cambiamenti rilevanti in ordine al servizio**, come l'attuazione di finalità aggiuntive

IL CONTENUTO DEI CONTRATTI

14. Previsione di attività di **logging** ed **auditing** delle operazioni di trattamento dei dati personali svolte dal fornitore e dai sub contraenti

15. **Obbligo di notifica al cliente di eventuali richieste di divulgazione** di dati personali svolte da un'autorità di contrasto, salvo il caso in cui la segretezza sia prescritta per legge

16. **Garanzia di conformità alla vigente legislazione** nazionale ed internazionale dell'organizzazione interna e del sistema di trattamento utilizzato dal fornitore e dai suoi sub fornitori

17. **Diritto al risarcimento del danno** subito in conseguenza dell'illegittimo trattamento di dati personali

Le misure tecniche ed organizzative

Ai sensi dell'art. 17, par. 2 Dir. 95/46/CE, il **cliente cloud**, in qualità di **titolare del trattamento**, ha la piena responsabilità della scelta di fornitori che adottino le **misure di sicurezza tecniche ed organizzative** adeguate a proteggere i dati, garantendone:

- **la disponibilità (accesso tempestivo** ed **affidabile**, prevenzione di perdita accidentale di connettività, attacchi informatici, guasti accidentali dell'hardware e altri problemi infrastrtutturali)
- **l'integrità** (in relazione all'impossibilità di **alterazione accidentale o volontaria** dei dati, durante le operazioni di trattamento, archiviazione o trasmissione)
- **l'autenticità** (mediante meccanismi di **autenticazione crittografica**, quali codici di autenticazione di messaggi o firme)

Le misure tecniche ed organizzative

- **la riservatezza** (criptaggio dei dati, meccanismi di autorizzazione ed autenticazione, obblighi di riservatezza per dipendenti del fornitore e degli eventuali subfornitori)
- **l'isolamento** ("limitazione della finalità" e prevenzione del rischio di divulgazione e trattamento per scopi illegittimi)
- **la portabilità** (adozione di formati standard ed interfacce che facilitano l'interoperabilità, al fine di evitare il rischio di lock-in)

Scegliere un cloud provider di qualità: i consigli operativi del Garante
Il Garante consiglia di fare una valutazione dei rischi, costi e benefici preventiva rispetto all'utilizzo di servizi cloud.
Valutare il **tipo di cloud** e il **modello di servizio** più adatti alle proprie esigenze ed al **tipo di dati** che si ha la necessità di esternalizzare.
La voce «risparmio» non deve essere l'unico fattore di scelta.
Sfruttare l'ampiezza del mercato, scegliendo tra differenti provider.

OSSERVATORI.NET digital innovation

La mini guida del Garante del giugno 2012 "Proteggere i dati per non cadere dalle nuvole"

Il decalogo del Garante
1. Effettuare una **verifica sull'affidabilità dei fornitori**
2. Privilegiare i servizi che favoriscono **l'interoperabilità** e la **portabilità** dei dati
3. Assicurarsi la **disponibilità** dei dati in caso di necessità (continuità operativa e disaster recovery)
4. **Selezionare i dati** da inserire nella nuvola
5. **Non perdere di vista i dati**
6. Informarsi su **dove risiederanno** concretamente i dati
7. Porre attenzione alle **clausole contrattuali**
8. Verificare il **rispetto delle finalità, dei tempi e delle modalità di conservazione** dei dati
9. Esigere adeguate **misure di sicurezza**
10. **Formare adeguatamente il personale**

Il trasferimento dei dati personali all'estero

- **Trasferimento di dati all'interno dell'Unione Europea**
  Le disposizioni del Codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

- **Trasferimento di dati al di fuori dell'Unione Europea**
  In caso di trasferimento anche temporaneo, con qualsiasi forma o mezzo, di dati personali verso paesi non appartenenti all'Unione Europea si applicano gli articoli 43 e ss del D.lgs 196/2003.

- **La direttiva 95/46/CE si applica a tutti gli Stati membri dello Spazio Economico Europeo che comprende tutti gli Stati membri dell'Unione Europea più Norvegia, Islanda e Liechtenstein.**

Il trasferimento dati all'estero

Il trasferimento anche temporaneo di dati personali verso un Paese terzo è, in linea di massima, **vietato**, a meno che l'ordinamento del Paese di destinazione o di transito non assicuri **un livello di tutela adeguato** (art. 25, comma 1 Direttiva 95/46 – Art. 44 D.Lgs. 196/2003)

In deroga a tale principio, **il trasferimento dei dati** verso società che hanno sede al di fuori dell'UE o del SEE **è consentito**:

- nelle **ipotesi espressamente previste** agli artt. 26, comma 1 Direttiva Privacy e 43 Codice Privacy (consenso dell'interessato e specifiche finalità del trattamento;
- quando è **autorizzato la Garante sulla base di adeguate garanzie per i diritti dell'interessato** (art. 26, comma 2 Direttiva Privacy e art. 44 Codice Privacy).

I trasferimenti consentiti (art. 43 D.Lgs. 196/2003)

Il **trasferimento di dati personali** verso un paese terzo **è consentito** quando:

a) l'interessato ha manifestato il proprio **consenso espresso** o, se si tratta di dati sensibili, in forma scritta;
b) è necessario per **l'esecuzione di obblighi derivanti da un contratto** del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
c) è necessario o prescritto dalla legge per la **salvaguardia di un interesse pubblico rilevante** individuato con legge o con regolamento;
d) è necessario per la **salvaguardia della vita o dell'incolumità fisica** dell'interessato o di un terzo;
e) è necessario ai fini dello **svolgimento delle investigazioni difensive** di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per **far valere o difendere un diritto in sede giudiziaria**, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
f) è effettuato in **accoglimento di una richiesta di accesso ai documenti amministrativi**, ovvero di una richiesta di **informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque**, con l'osservanza delle norme che regolano la materia;
g) è necessario per **esclusivi scopi scientifici, statistici, storici**.

I trasferimenti consentiti (art. 43 D.Lgs. 196/2003)

Bisogna ricordare che l'Art. 29 WP ha adottato un parere nel quale afferma che **le ipotesi di esenzione** che consentono agli esportatori di trasferire dati al di fuori dell'UE senza fornire garanzie aggiuntive **si applicano solo quando i trasferimenti non sono ricorrenti, né massicci o strutturali**.

Ciò fa sì che la possibilità di applicare le deroghe previste dall'art. 43 Codice Privacy sia quasi impossibile nel contesto del cloud computing.

Altri trasferimenti consentiti (art. 44 D.Lgs. 196/2003)

Il trasferimento dei dati verso società che hanno la loro sede al di fuori della UE o del SEE è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

a) Individuate dal Garante:
- in relazione alle **garanzie prestate con un contratto**;
- mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo (cc.dd. **Binding Corporate Rules**).

b) Individuate dalla Commissione Europea mediante decisioni con cui:
- la Commissione Europea constata che un Paese non appartenente all'UE o al SEE garantisce un livello di protezione adeguato (cc.dd. **decisioni di adeguatezza)**;
- la Commissione Europea constata che alcune clausole contrattuali offrono garanzie sufficienti (cc. dd. **clausole contrattuali standard**).

Autorizzazioni del Garante per il trasferimento dei dati sulla base delle garanzie offerte dal contratto

In questo caso il Garante deve adottare un'autorizzazione specifica al trasferimento

Sostanzialmente il Titolare del trattamento che intende adottare un contratto non basato su clausole contrattuali tipo deve richiedere al Garante un'autorizzazione al trasferimento dei dati verso paesi che non garantiscono un livello adeguato di protezione.

Autorizzazioni del Garante basate sulle Binding Corporate Rules

Le BCR sono uno strumento volto a consentire il flusso transfrontaliero di dati tra **società facenti parte dello stesso gruppo d'impresa**, tutte tenute al rispetto dei principi vincolanti fissate attraverso di esse.

Semplificazione degli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali.

L' autorizzazione del Garante è rilasciata dietro espressa richiesta della società interessata, con riferimento a trasferimenti di dati personali dall'Italia verso Paesi terzi che si svolgano nel rispetto di quanto stabilito all'interno del testo di BCR e per le sole finalità ivi indicate.

La **procedura di definizione ed approvazione del testo delle BCR** – elaborata dall'art. 29 WP – si articola in **due fasi**:

1. **Una fase a carattere «europeo»**, coordinata da una sola Autorità (c.d. *lead Authority*) che dialoga con la società capogruppo, in rappresentanza di tutte le altre DPA dei Paesi interessati dal trasferimento;
2. **Una fase a carattere «nazionale»**, mediante la quale il Garante procede al rilascio di un'autorizzazione nazionale al trasferimento dei dati personali oggetto del testo delle BCR (ad oggi il Garante ha emanato undici autorizzazioni di trasferimento dei dati basate sulle BCR).

I contenuti delle Binding Corporate Rules

Il testo di BCR contiene i principi fondamentali in materia di protezione dei dati personali sanciti dal Codice Privacy e dalla Direttiva 95/46/CE secondo le indicazioni fornite dall'art. 29 WP.

In particolare, l'art. 29 WP **ha individuato con vari documenti gli specifici requisiti che le regole di condotta devono soddisfare al fine di consentire ai gruppi multinazionali d'impresa** di ottenere le necessarie autorizzazioni nazionali al trasferimento dei dati all'interno del gruppo, tra cui: i principi di correttezza e legittimità del trattamento, di finalità, necessità e proporzionalità dei dati, l'obbligo del titolare di rilasciare idonea informativa all'interessato, i diritti dell'interessato, le misure di sicurezza prescritte dalla legge, il diritto dell'interessato ad ottenere il risarcimento del danno connesso al mancato rispetto delle BCR da parte di una società del gruppo (c.*d. clausola del terzo beneficiario*).

Oneri ulteriori, inoltre, sono imposti al gruppo multinazionale d'impresa che deve garantire tra l'altro: la predisposizione di un programma di training del personale in materia di protezione dei dati personali; l'implementazione di un meccanismo di gestione del contenzioso e delle segnalazioni connesse alle BCR; la conduzione periodica di audit al fine di verificare il rispetto delle BCR da parte delle società del gruppo; la creazione di un network di *privacy officers* o di uno staff che si occupi di monitorare il rispetto delle BCR e di gestire le segnalazioni degli interessati.

I trasferimenti autorizzati sulla base delle decisioni di adeguatezza della Commissione Europea

La Commissione europea può stabilire, sulla base di un procedimento che prevede, fra l'altro, il parere favorevole del **Gruppo ex Art. 29** della **Direttiva 95/46/CE**, che il livello di protezione offerto in un determinato Paese è adeguato e che pertanto è possibile trasferirvi dati personali.

Ad oggi i Paesi che sono stati riconosciuti dalla Commissione Europea come Paesi terzi che garantiscono un livello adeguato di protezione dei dati sono: Svizzera, Andorra, Argentina, Canada, Israele, Isola di Man, Isole Fær Øer, Baliato di Jersey e Baliato di Guernsey, Nuova Zelanda, Uruguay.

Il Garante adotta di regola delle autorizzazioni generali al trasferimento dei dati verso i paesi che sono stati riconosciuto dalla Commissione Europea come un paese terzo che garantisce un livello adeguato di protezione dei dati.

I trasferimenti autorizzati sulla base delle decisioni di adeguatezza della Commissione Europea

Per quanto riguarda gli Stati Uniti esiste l'accordo del c.d. **Safe Habor** (Decisione della Commissione Europea n. 2000/520/CE del 26 luglio 2000) che prevede che le società statunitensi si iscrivano alla Safe Harbor List tenuta dal Dipartimento del Commercio degli Stati Uniti ed in questo modo dichiarino di **rispettare i principi contenuti nella direttiva 95/46/CE**

Pertanto prima di trasferire i dati verso una società statunitense è necessario verificare se la stessa è iscritta nella Safe Harbor List

Nel nostro Paese il *Safe Harbor* è stato recepito con deliberazione del Garante Privacy n. 36 del 10 ottobre 2001 "Autorizzazione al trasferimento verso gli Stati Uniti d'America".

Tuttavia, secondo il parere del Gruppo di lavoro ex art. 29 il Gruppo di lavoro ex art 29 ritiene che **le società che esportano dati non dovrebbero semplicemente basarsi sulla dichiarazione dell'importatore dei dati in merito alla certificazione Safe Harbor**.
E' necessaria **la prova dell'esistenza delle autocertificazioni "Safe Harbor" ed è necessario richiedere che venga dimostrata l'osservanza dei relativi principi**.

I trasferimenti autorizzati sulla base delle clausole contrattuali tipo

Sono state individuate dalla Commissione europea delle clausole contrattuali tipo per il trasferimento da:

- Titolare del trattamento a Titolare del trattamento con le decisioni 2001/497/CE del 15 giugno 2001 e 2004/915/CE del 27 dicembre 2004
- Titolare del trattamento a Responsabile del trattamento con la decisione 2010/87/UE del 5 febbraio 2010

Il Titolare del trattamento che trasferisce i dati verso un paese che non garantisce un livello adeguato di protezione dei dati deve stipulare un "*data transfer agreement*" basato sulle clausole contrattuali tipo adottate dalla Commissione Europea.

Il Gruppo di Lavoro ex art 29 della Dir 95/46/CE ha chiarito che le clausole contrattuali possono essere adottate soltanto per trasferimenti punto-punto e non possono essere utilizzate in caso di adozione di contratti multilaterali.

OSSERVATORI.NET digital innovation

Riepilogando….

Quali interrogativi porsi (e porre ai fornitori)	Esigenze minime di tutela
Quali sono le **misure di sicurezza adottate dal fornitore** per proteggere i dati? È possibile che i **dati sul cloud possano essere persi o distrutti**?	Adozione di adeguate misure di sicurezza e sistemi di logging
In caso di problemi al collegamento Internet, è comunque possibile continuare a usufruire dei servizi senza l'accesso al cloud? **In quanto tempo può essere ripristinato il sistema**? Esistono piani di emergenza per i servizi essenziali?	Piani di emergenza, continuità operativa, disaster recovery
Chi è il **reale fornitore del servizio che si sta acquisendo**? Si tratta di una singola società o di un consorzio di imprese?	Trasparenza sulla catena dei subfornitori
In quale Stato sono conservati i dati caricati sulla "nuvola"? È possibile scegliere di usufruire di server collocati solo in territorio nazionale o in Paesi dell'Unione europea?	Adempimenti relativi al flusso transfrontaliero dei dati
La tecnologia utilizzata dal fornitore di cloud è di tipo "**proprietario**"? **I dati possono essere esportati facilmente?**	Interoperabilità, portabilità, no lock-in dei dati
Esistono **garanzie di riservatezza** per i nostri dati nel caso in cui un concorrente condivida gli stessi servizi cloud?	Clausole di riservatezza
Nel caso in cui si accerti una violazione o la perdita dei dati, **il fornitore garantisce un pronto risarcimento del danno**?	Attenta valutazione delle clausole contrattuali

Grazie per l'attenzione!

Per domande ed approfondimenti:

annamaria.italiano@p4i.it