Studio Mazzolari
Privacy Consulting - MILANO

MULTINAZIONALI E FLUSSI DI DATI PERSONALI

FUORI DAL TERRITORIO DELL'UNIONE EUROPEA

Milano, 21 settembre 2011

PREMESSA

L'approfondimento di questo Post riguarda la scelta già operata da Multinazionali quali eBay, General Electric Company, Philips, Accenture Limited, Hyatt Hotel Corporation, JPMorgan Chase & Co, British Petroleum plc, Michelin e altre, relativa alla propria Compliance alla normativa europea che regolamenta il trattamento dei dati personali: qual è la più efficiente soluzione giuridica per regolarizzare i flussi di informazioni in partenza da un Membro stabilito sul territorio europeo verso un altro Membro extra UE?
Bene, andiamo a fare chiarezza sul tema.

IL FLUSSO DI DATI PERSONALI INTRA UE

Il Decreto Legge 70/2011 (Decreto Sviluppo) ha introdotto un'importante semplificazione in merito al ***flusso di dati infragruppo tra membri stabiliti sul territorio europeo***. Per la precisione all'Art. 24 rubricato "Casi nei quali può essere effettuato il trattamento senza consenso" del Codice Privacy è stato aggiunta la lettera i-ter) la quale estende le eccezioni all'obbligo del consenso da parte dell'Interessato per il trattamento dati comuni, quando il trattamento:

- ✓ riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti:
- ✓ ha ***finalità amministrativo contabili***, come definite all'articolo 34, comma 1-ter[1], purché queste finalità siano previste espressamente con ***determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13***.

[1] Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

Pertanto: il flusso di dati personali di tipo comune relativo a finalità amministrativo-contabili tra società appartenenti al medesimo Gruppo stabilite sul territorio dell'Unione Europea può lecitamente avere luogo solo dopo idonea integrazione dell'Informativa da rendere agli Interessati

I FLUSSI DI DATI PERSONALI EXTRA UE: INQUADRIAMO LA QUESTIONE

Il Codice Privacy (DLgs 196/2003) disciplina il trattamento dei dati anche dal punto di vista del loro trasferimento all'estero, affermando il principio secondo cui, mentre all'interno dell'Unione europea è prevista come regola generale la libera circolazione (non soggetta a restrizioni salvo che in caso di eventuali fenomeni elusivi di garanzie), ***il trasferimento di informazioni personali verso Paesi terzi è invece possibile, sempre come regola generale, solo se il Paese di destinazione garantisce un livello di protezione adeguato secondo la valutazione effettuata dalla Commissione europea*** (artt. 42 e 44 Codice cit.).
Poiché diversi Paesi terzi non offrono tale protezione, in attuazione di quanto disposto dalla direttiva comunitaria in materia (n. 95/46/Ce del 24 ottobre 1995), sono previste alcune ***condizioni equipollenti in base alle quali il trasferimento può avvenire comunque***, ad esempio perché vi è il consenso dell'interessato, od occorre eseguire obblighi contrattuali o salvaguardare un interesse pubblico rilevante (art. 43 Codice cit.).
Tra queste condizioni equipollenti vi è anche il caso nel quale il trasferimento può essere autorizzato dal Garante in presenza di garanzie individuate dalla stessa Autorità come "adeguate" in rapporto ai diritti degli interessati (art. 44, comma 1, lett. a)).
Su queste basi, l'esperienza di collaborazione con la Commissione europea e con le autorità garanti degli altri Paesi dell'Unione ha già individuato alcuni strumenti utili basati su ***clausole contrattuali standard approvate con decisione della Commissione europea*** (art. 26, par. 4 dir. n. 95/46/Ce cit.).
In particolare, sono stati predisposti su scala europea alcuni contratti-tipo che hanno permesso di regolare in modo uniforme, e tendenzialmente agevole, diversi flussi di dati verso

Paesi terzi nei quali operino ***titolari del trattamento autonomi*** rispetto al soggetto esportatore, oppure strutture che agiscono in funzione strumentale quali ***"responsabili" del trattamento***.

GLI STATI UNITI E IL SISTEMA DEL SAFE HARBOR

Per quanto riguarda il trasferimento di dati negli U.S.A., il 26 luglio 2000 la Commissione europea ha adottato una decisione con la quale riconosce che il dispositivo di "*Safe Harbor*", approntato dalla Commissione federale per il commercio degli Stati Uniti (Federal Trade Commission), assicura un adeguato livello di protezione dei dati personali trasferiti dall'Unione europea.

Il "*Safe Harbor*" costituisce un ***insieme di principi a garanzia del trattamento dei dati personali uniti alla previsione di alcuni sistemi per assicurare il rispetto di tali principi***.

L'adesione al "*Safe Harbor*" è facoltativa per le imprese americane, ma le regole in esso contenute vincolano le imprese aderenti; il loro rispetto è affidato alla *Federal Trade Commission* e, per le compagnie aeree, all'Amministrazione dei trasporti.

La decisione comunitaria è il frutto di due anni di intenso negoziato tra le parti volto ad evitare che il trasferimento di dati personali verso gli U.S.A. potesse essere limitato o sottratto a garanzie in seguito all'entrata in vigore della direttiva n. 95/46/CE.

I cittadini dell'Unione europea che intendano reclamare per il trattamento effettuato da un partecipante al "*Safe Harbor*" possono rivolgersi ad un'autorità indipendente di composizione di controversie: ogni organismo statunitense aderente al "*Safe Harbor* " deve indicare l'autorità con la quale si impegna a collaborare. In vari casi è pure possibile agire davanti a giudici statunitensi, in base a norme dell'ordinamento d'oltreoceano che non permettono "dichiarazioni false", quali appunto quelle di un'impresa che dichiari di aderire ad una certa politica di protezione dei dati personali successivamente non rispettata.

LE "CLAUSOLE CONTRATTUALI TIPO"

In tutti gli altri casi in cui il Paese terzo di esportazione non è gli Stati Uniti, un elevato numero di imprese attive su scala internazionale si sono avvalse delle Clausole Contrattuali tipo.
L'esperienza applicativa ha portato però a evidenziare alcune difficoltà che incontrano, soprattutto, società operanti all'interno di Gruppi multinazionali, nell'applicare le predette opportunità in Europa con un approccio distinto da Paese a Paese.
Per tali Gruppi, anche l'impiego di modelli contrattuali standardizzati viene infatti avvertito, a volte, come farraginoso, in quanto ***ciascuna società stabilita all'interno dello Spazio economico europeo e appartenente ad un medesimo Gruppo multinazionale deve comunque includere le garanzie previste dai predetti schemi tipo in un suo contratto con le società del Gruppo situate in Paesi terzi.***
Pertanto, il Working Party che riunisce le autorità garanti d'Europa, istituito ai sensi dell'art. 29 della direttiva 95/46/Ce (c.d. Working Party art. 29), ha preso in considerazione ulteriori strumenti, rispetto a quello contrattuale, che possano assicurare anch'essi un livello adeguato di protezione per i diritti degli interessati, con particolare riguardo al trasferimento all'estero dei dati personali nell'ambito dei Gruppi multinazionali.
Il Working Party ha operato alcune prime valutazioni con riserva di eventuali situazioni specifiche connesse a singole realtà nazionali, ravvisando un'interessante prospettiva di lavoro nelle regole di comportamento che una società capogruppo può impartire, generalmente all'interno di appositi codici di condotta interni al Gruppo multinazionale e resi vincolanti per tutte le società ad esso appartenenti.
Tali regole, ormai conosciute nella prassi applicativa come ***Binding Corporate Rules (BCRs)*** sono state ritenute come uno strumento astrattamente idoneo ad assicurare un livello adeguato di protezione per i diritti degli interessati, compatibile con la disciplina contenuta nella direttiva 95/46/Ce.
Il Working Party ha precisato che le ***BCRs*** possono essere impiegate utilmente sempreché siano effettivamente vincolanti in un duplice senso:

- ✓ ***all'interno del Gruppo di società*,** grazie anche alla previsione di "sanzioni private" nei confronti degli incaricati operanti presso le società interessate;
- ✓ ***all'esterno del Gruppo di società***, al fine di consentire l'esercizio dei diritti risultanti dalle regole di condotta interne al Gruppo agli interessati cui si riferiscono i dati trasferiti.

LA MODIFICA ALL'ART. 44 DLGS 196/2003

Per garantire l'accesso allo strumento dei BCRs da parte di Soggetti giuridici stabiliti sul territorio italiano, il DL 25 giugno 2008 ha modificato la lettera a) dell'Art. 44 del Codice Privacy rubricato "Altri trasferimenti consentiti" aggiungendo il seguente periodo:
Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando e autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:
a) individuate dal Garante anche in relazione a garanzie prestate con un contratto ***o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo Gruppo. L'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice, anche in ordine all'inosservanza delle garanzie medesime***

I BCRS (BINDING CORPORATE RULES)

Le "norme vincolanti d'impresa" sono pertanto veri e propri codici di condotta elaborati nell'ambito di un Gruppo di imprese e validi per tutte le imprese che di tale Gruppo fanno parte.
La finalità è quella di ***offrire garanzie sufficienti ai fini del trasferimento di dati verso Paesi terzi che non dispongono di un livello adeguato di protezione dei dati personali***. In

particolare, per quanto riguarda il trasferimento fra società appartenenti ad uno stesso Gruppo multinazionale.

La possibilità di utilizzare "norme vincolanti di impresa" per i trasferimenti di dati personali da imprese europee ad altre società appartenenti allo stesso Gruppo multinazionale presuppone almeno che:

- ✓ le norme d'impresa siano ***effettivamente vincolanti***;
- ✓ si tratti, appunto, di norme d'impresa, ossia di norme elaborate da un Gruppo multinazionale ed effettivamente valide per tutte le società che di tale Gruppo fanno parte. Ciò significa, in pratica, che ***per il trasferimento di dati verso soggetti terzi extra-Gruppo, le norme d'impresa non possono avere, ovviamente, alcuna validità*** e, dunque, si dovrà ricorrere, eventualmente, ad altri strumenti contrattuali come le clausole standard.

Tra il 2003 e il 2008, il Working Party ex art. 29 individua gli specifici requisiti che i BCRs devono soddisfare al fine di consentire ai Gruppi multinazionali d'impresa, che intendano adottarle, di ottenere le necessarie autorizzazioni nazionali al trasferimento transfrontaliero dei dati all'interno del Gruppo, attraverso i seguenti documenti:

- ✓ WP 74 del 3 giugno 2003,
- ✓ WP 108 del 14 aprile 2005
- ✓ WP 133 del 10 gennaio 2007
- ✓ WP 153 del 24 giugno 2008

LA APPLICATION FORM PER L'APPROVAZIONE DEI BCRS

La procedura di richiesta di approvazione dei BCRs è analiticamente indicata nel WP 133.

Il Gruppo richiedente deve compilare *un'Application form* che consta di due Parti con rispettive Sezioni:

1. ***Applicant Information***

1.1. *Struttura e Contatti* del richiedente e del Gruppo;

1.2. *Breve descrizione del flusso di dati*;

1.3. Indicazione della *Lead Data Protection Authority*[2] .

2. ***Background Paper***
   - ***2.1.*** *La natura vincolante delle BCRs* (vincolanti in un duplice senso: ***all'interno del Gruppo di società,*** grazie anche alla previsione di "sanzioni private" nei confronti degli incaricati operanti presso le società interessate; ***all'esterno del Gruppo di società***, al fine di consentire l'esercizio dei diritti risultanti dalle regole di condotta interne al Gruppo agli interessati cui si riferiscono i dati trasferiti);
   - ***2.2.*** *Effettività* (verifica della compliance, attraverso, ad esempio, strumenti quali programmi di audit, attività di corporate governance, compliance departments, etc.)
   - ***2.3.*** *Cooperazione con le DPAs* (Data Protection Authorities);
   - ***2.4.*** *Descrizione dei trattamenti e dei flussi di dati personali*;
   - ***2.5.*** *Meccanismi di Reporting e Registrazione di cambiamenti*;
   - ***2.6.*** *Misure di sicurezza adottate a protezione dei dati personali*;
   - ***2.7.*** *Allegato 1: Copia del Formal Binding Corporate Rules*.

RISPOSTE ALLA DOMANDE PIÙ FREQUENTI (FAQS)

L'Article 29 Working Party, nel giugno del 2008, è intervenuto per dirimere i seguenti dubbi ricorrenti:

1 - Le BCRs si devono applicare a tutti i dati personali trattati dal Gruppo?

No, le BCRs sono uno strumento legale per fornire una protezione adeguata ai dati personali, così come individuati dalla Direttiva 95/46/EC, nei loro ***trasferimenti al di fuori***

[2] La ***Lead DPA*** è l'authority che si farà carico di coordinare l'approvazione della richiesta con tutte le altre DPAs degli altri Stati all'interno della UE che vengono indicati nell'application come Stati all'origine dei trasferimenti dei dati personali dai membri del Gruppo verso stati terzi

dell'Unione europea verso paesi che non sono considerati fornire un livello adeguato di protezione.

Altri dati personali trattati dal Gruppo, che non vengono trattati all'interno della Unione Europea UE, non devono essere considerati dalle BCRs.

Tuttavia, si raccomanda che i Gruppi multinazionali, utilizzando le BCRs, adottino un insieme omogeneo di politiche globali o regole in modo da proteggere tutti i dati personali trattati. Avere un unico insieme di norme creerà un sistema più semplice ed efficace, più facile da implementare da parte del personale e da comprendere da parte degli Interessati. Le aziende possono vedere incrementato il proprio indice di gradimento e fidelizzazione grazie ad un impegno fermo per un alto livello di privacy verso i soggetti interessati indipendentemente dalla loro ubicazione e dalle disposizioni di legge in tutte le giurisdizioni.

2 - Le BCRS si applicano anche a Responsabili del trattamento che non fanno parte del Gruppo?

No, solo i Responsabili che fanno parte del Gruppo e che trattano dati per conto di altri membri del Gruppo dovranno rispettare le BCRs come membri del Gruppo.

Le BCRs potrebbero contenere regole particolari rivolte a membri del Gruppo nella loro veste di Responsabili del trattamento come strumento per soddisfare i requisiti di cui agli articoli 16 e 17 della direttiva 95/46/EC[3].

[3] **RISERVATEZZA E SICUREZZA DEI TRATTAMENTI**
Articolo 16
Riservatezza dei trattamenti
L'incaricato del trattamento o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento non deve elaborare i dati personali ai quali ha accesso, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi legali.
Articolo 17
Sicurezza dei trattamenti
1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.
Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere.
2. Gli Stati membri dispongono che il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure.
3. L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente:
- che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento;
- che gli obblighi di cui al paragrafo 1, quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.

Responsabili che non fanno parte del Gruppo e agiscono per conto di un membro del Gruppo non sono tenuti a essere vincolati dalle BCRs. Tuttavia, questi soggetti dovrebbe agire sempre e solo secondo le istruzioni del Titolare del trattamento e dovrebbero essere vincolati da contratto o altro atto giuridico in linea con le disposizioni degli articoli 16 e 17 della direttiva del'Unione Europea.

Se i Responsabili che trattano i dati non fanno parte del Gruppo e sono stabiliti al di fuori dell'UE, i membri del Gruppo dovranno inoltre conformarsi agli articoli 25 e 26 della direttiva 95/46/CE relativi ai flussi transfrontalieri di dati e garantire un adeguato livello di protezione[4]. Per esempio, l'azienda può cercare di garantire la compliance con

4. A fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti concernenti le misure di cui al paragrafo 1 sono stipulati per iscritto o in altra forma equivalente.

[4] **TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI**
Articolo 25
Principi
1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.
2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.
3. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.
4. Qualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.
5. La Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4.
6. La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.
Articolo 26
Deroghe
1. In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi del'articolo 25, paragrafo 2 può avvenire a condizione che:
a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure
b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure
d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria, oppure
e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.
2. Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il

mezzi contrattuali facendo uso, ad esempio, delle clausole contrattuali tipo adottato dalla Commissione europea per i trasferimenti di un Responsabile del trattamento al di fuori dell'UE oppure sottoponendo i Responsabili del trattamento alle disposizioni della BCRs relativamente ai loro dati.

3 - Qualora la violazione dei BCRs si verifichi al di fuori dell'UE quale membro del Gruppo è responsabile?

Indipendentemente dall'esistenza di una responsabilità ai sensi della direttiva 95/46/EC per l'entità che esporta dati personali dall'UE, le BCRs devono prevedere una ***entità all'interno dell'UE che accetti la responsabilità per eventuali violazioni delle regole da parte di qualsiasi membro del Gruppo al di fuori dell'UE.*** Questa responsabilità ha solo bisogno di estendersi ai dati trasferiti dalla UE secondo le BCRs.

Il WP74 prevede che nella maggior parte dei casi sia la sede del Gruppo (***Headquarter***), se stabilita nell'UE, a farsi carico di tale responsabilità.

Qualora la sede del Gruppo sia stabilita al di fuori dell'UE, il WP74 consente al Gruppo di ***nominare un membro idoneo nella UE che si faccia carico della responsabilità per violazione delle regole al di fuori dell'UE***.

Questa responsabilità include, ma non solo, il pagamento di eventuali danni derivanti dalla violazione delle BCRs da parte di qualsiasi membro al di fuori dell'UE vincolato alle regole. Tuttavia, per alcuni Gruppi con strutture particolarmente complesse, non sempre è possibile imporre ad un ente specifico di farsi carico di tutte le responsabilità per qualsiasi violazione al di fuori della UE. In questi casi, il Working Party accetta che, qualora il Gruppo sia in grado di dimostrare il motivo per il quale non sia possibile nominare una singola entità all'interno dell'UE, si possano proporre altri meccanismi di responsabilità che si adattano meglio

responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate.
3. Lo Stato membro informa la Commissione e gli altri Stati membri in merito alle autorizzazioni concesse a norma del paragrafo 2.
In caso di opposizione notificata da un altro Stato membro o dalla Commissione, debitamente motivata sotto l'aspetto della tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, la Commissione adotta le misure appropriate secondo la procedura di cui all'articolo 31, paragrafo 2.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.
4. Qualora la Commissione decida, secondo la procedura di cui all'articolo 31, paragrafo 2, che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui al paragrafo 2, gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.

all'organizzazione.

Una possibilità sarebbe quella di creare un meccanismo comune di responsabilità tra gli importatori e gli esportatori di dati così come individuato nelle Clausole Contrattuali Standard UE 2001/497/CE del 15 giugno 2001 oppure definire uno schema alternativo di responsabilità sulla base di *due diligence obligations*, così come prescritto nelle Clausole Contrattuali Standard UE 2004/915/CE.

Un'ultima possibilità, specificamente dedicata ai trasferimenti effettuati da Titolari del trattamento a Responsabili del trattamento è l'applicazione del meccanismo di responsabilità delle Clausole Contrattuali Standard 2002/16/CE del 27 dicembre 2001.

Le Autorità per la protezione dei dati personali possono accettare le soluzioni alternative di cui sopra relative alla responsabilità caso per caso, laddove vengano fornite sufficienti e idonee garanzie da parte del richiedente. Qualora un meccanismo alternativo venga utilizzato, è importante specificare che i soggetti interessati saranno assistiti nell'esercizio dei propri diritti e non svantaggiati o ostacolati in alcun modo.

4 – Le BCRs devono contenere sempre un diritto per l'interessato di presentare un ricorso dinanzi all'autorità per la protezione dei dati in caso di violazione delle BCRs stesse?

Sì, nonostante il fatto che in alcuni casi le regole o i diritti del terzo beneficiario possano essere limitati ai soli dati provenienti dall'UE e gli individui abbiano già un diritto nella loro normativa nazionale per ricorrere contro il soggetto esportatore dei dati davanti all'autorità per la protezione dei dati personali, è importante ***riconoscere il diritto di presentare un reclamo a norma delle BCRs per una violazione delle norme nel loro complesso da parte di qualsiasi membro del Gruppo.***

5 – Le informazioni circa i diritti del terzo beneficiario devono essere rese disponibili agli Interessati che ne beneficiano?

Sì, WP74 richiede che sia le BCRs sia le modalità per proporre reclamo e cercare un rimedio a una violazione delle norme debbano essere facilmente accessibili al soggetto interessato.

L'esistenza di diritti del terzo beneficiario e il loro contenuto è un'opzione importante per un Interessato quando si considerano i rimedi a sua disposizione.

Alcune aziende hanno deciso per motivi legittimi, di non includere la clausola dei diritti del terzo beneficiario nel documento chiave delle BCRs ma di impostare tali diritti in un documento separato. ***Nei casi in cui i diritti siano in un documento separato questi dovrebbero essere resi trasparenti e facilmente accessibili per le persone interessate che beneficiano di tali diritti.***

6 – Le BCRs devono descrivere le finalità dei trattamenti effettuati dal Gruppo? A quale livello di dettaglio?

Si, una descrizione del trattamento dovrà essere inclusa nelle BCRs e dovrà essere ***sufficientemente dettagliata per consentire alle Autorità per la protezione dei dati personali (DPAs) di valutare se il livello di protezione di dati personali del Gruppo sia adeguato***.

Questa descrizione deve essere chiara e precisa e specificare le finalità principali del trattamento in modo dettagliato (ad esempio, descrivendo se includono la gestione delle risorse umane, l'esecuzione del processo di business e di gestione, la sicurezza, etc.), in particolare se i dati personali sono trattati anche per scopi di marketing diretto.

Paolo Mazzolari - Privacy Consulting and Training

p.mazzolari@mazzolari.eu