Brain IT s.r.l.
Corso Trieste 61
00198 Roma
P.IVA 15082451004

Trasferimento di dati personali all'estero
BCR

Le **Binding Corporate Rules** sono uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-UE). Le Bcr si concretizzano in una serie di **clausole** che fissano i principi **vincolanti** al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo, allo **scopo** di semplificare gli oneri amministrativi a carico delle società multinazionali con riferimento ai flussi intra-gruppo di dati personali (**art. 47 GDPR**).

Sommario

Trasferimento di dati personali all'estero

Per trasferimento del dato si intende la comunicazione di informazioni afferenti al personale dipendente fra le sedi italiane o comunque europee e sedi estere di un gruppo multinazionale strutturato.

Il problema principale che ha investito questa tipologia di trasferimenti, era rappresentato dalle differenti legislazioni con cui ci si doveva confrontare al momento del trasferimento dei dati, qualora protagonista del trasferimento medesimo fosse stata una struttura operativa che doveva far elaborare i suoi dati ad una sua società dislocata fuori dai confini europei.

Ci si trovava di fronte dunque ad una sorta di patchwork legislativo che limitava fortemente il dialogo tra il titolare e il responsabile del trattamento. Sul punto infatti, le disposizioni comunitarie contenute nel Direttiva 95/46 stabilivano che un trasferimento di questo tipo poteva trovare applicazione, solo allorché lo stato di destinazione presentasse delle garanzie di tutela per il diritto alla protezione dei dati personali che rispettassero gli standard presenti all'interno della Comunità Europea.

Se così non fosse, il trasferimento dei dati personali poteva avere luogo solo qualora i soggetti che ponevano in essere il trasferimento e il trattamento dei dati fornissero delle adeguate garanzie per la tutela del diritto alla protezione dei dati personali.

In data 10 novembre 2020 il Comitato europeo per la protezione dei dati personali ha adottato le raccomandazioni sulle misure da integrare in occasione del trasferimento extra UE per garantire la conformità con il livello di protezione dei dati personali previsto nell'UE: una vera e propria roadmap in sei step per supportare i titolari e responsabili del trattamento.

Binding Corporate Rules, è un'espressione sempre più diffusa soprattutto a seguito del 'terremoto' Safe Harbor. Ne è stata sottolineata l'utilità di recente dallo stesso Garante per la protezione dei dati personali che ha ufficialmente dichiarato decaduta l'autorizzazione al trasferimento di dati verso gli Stati Uniti sulla base dell'accordo Safe Harbor.

Tale provvedimento non esclude infatti il poter dislocare dati oltreoceano, implica, tuttavia, che tutti gli attori coinvolti (società multinazionali, imprese italiane ed organizzazioni) ricorrano alle possibilità alternative già previste dalla normativa sulla protezione dei dati personali.

Naturalmente oltre alle indicazioni prima citate si deve sempre tener presente il GDPR che fornisce diversi strumenti per disciplinare i trasferimenti di dati dall'UE verso un paese terzo:

- talvolta, una decisione della Commissione europea («decisione di adeguatezza») può sancire che un determinato paese terzo è in grado di offrire un adeguato livello di protezione nel senso che è possibile trasferire dati a un'altra società in quel paese terzo senza che l'esportatore dei dati sia tenuto a fornire ulteriori garanzie o sia soggetto a condizioni supplementari. In altre parole, i trasferimenti verso un paese terzo «adeguato» saranno assimilati a una trasmissione di dati all'interno dell'UE;
- in mancanza di una decisione di adeguatezza, il trasferimento può aver luogo mediante la fornitura di garanzie adeguate e a condizione che le persone dispongano di diritti esecutivi e mezzi di ricorso efficaci. Tali garanzie adeguate comprendono, tra l'altro, quanto segue:
- nel caso di un gruppo di imprese o di gruppi di aziende che esercitano un'attività economica congiunta, le aziende possono trasferire dati personali sulla base delle cosiddette norme vincolanti d'impresa;
- accordi contrattuali con il destinatario dei dati personali, ad esempio utilizzando le clausole contrattuali tipo approvate dalla Commissione europea;

- l'osservanza di un codice di condotta o di un meccanismo di certificazione, unitamente all'ottenimento da parte del destinatario di impegni vincolanti ed esecutivi ad applicare le opportune garanzie per proteggere i dati trasferiti;
- infine, se è previsto un trasferimento di dati personali verso un paese terzo che non è soggetto a una decisione di adeguatezza e se mancano garanzie appropriate, può essere effettuato un trasferimento basato su una serie di deroghe per situazioni specifiche, ad esempio quando una persona ha esplicitamente acconsentito al trasferimento proposto dopo aver ricevuto tutte le informazioni necessarie sui rischi associati al trasferimento.

Il 22 maggio 2015, vede la luce il WP 204 ("Explanatory Document on the Processor Binding Corporate Rules") che al momento è l'ultimo lavoro elaborato dal Gruppo Ex Art. 29 che ha svilupapto e sviscerato il tanto discusso e delicato argomento giuridico e tecnico relativo ai trasferimenti di dati al di fuori del territorio europeo e degli strumenti di natura contrattuale che ne garantiscono la legittimità e l'affidabilità medesima.

Il concetto di trasferimento non è affatto chiaro e delineato né tantomeno definito dalle fonti europee (né tanto meno da quelle nazionali di recepimento) le quali ne vietano con assoluta determinatezza il verificarsi, salvo il ricorrere di ben precise condizioni.

L'articolo 26 della Direttiva Ce/95/46, recita che:

"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 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".

Definizioni utili

Di seguito un breve glossario per tenere semrpe sotto controllo le definizioni terminologiche utilizzate nel presente documento.

Paese terzo: è uno Stato non appartenente all´UE o allo Spazio Economico Europeo comprendente anche la Norvegia, l'Islanda e il Liechtenstein.

Organizzazione internazionale: ai sensi dell'art. 4.26) del GDPR, è un'organizzazione o un organismo di diritto internazionale pubblico ad essa subordinato o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Paese estero: un paese terzo o un'organizzazione internazionale.

Trasferimento: è un trattamento ed avviene se i dati del Titolare, soggetto alle disposizioni del GDPR, sono oggetto di un qualsiasi trattamento in un paese terzo o sono destinati ad esserlo dopo il trasferimento verso un Titolare, responsabile o destinatario stabilito fuori dell'ambito di applicazione del GDPR.

Trasferimento occasionale e non ripetitivo: si configurano tali quei trattamenti che possono ripetersi ma solo in circostanze non ordinarie e ad intervalli di tempo arbitrari, ovvero che sono conseguenti al manifestarsi di condizioni casuali o ignote e pertanto non hanno sicuramente cadenza regolare.

Trattamento: è definito dall'art. 4.2) del GDPR come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Comunicazione: è definita dal comma 4 dall'art. 2-ter del D. Lgs. n. 196/2003 come il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dell'Unione europea, dal Responsabile/Designato o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile/Designato, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.

Diffusione: è definita dal comma 4 dall'art. 2-ter del D. Lgs. n. 196/2003 come il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Adeguatezza: nel caso dei trasferimenti, indica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, ma che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione.

Decisione di adeguatezza: è la decisione della Commissione Europea, assunta a valle di una valutazione dell'adeguatezza del livello di protezione dei dati, che un paese terzo, un territorio, uno o più settori all'interno di un territorio o un'organizzazione internazionale garantiscono un livello di protezione adeguato per il trattamento dei dati personali.

Registro: un documento (in formato cartaceo o elettronico) in cui sono annotati con regolarità determinati elementi o particolari, oppure un elenco ufficiale riportante una serie di nomi o elementi.

Il contenuto

E' bene chiarire sin da subito che le BCR non si sostituiscano, non è il loro scopo, alla normativa in materia di protezione del dato personale, esse devono essere viste, scritte e vissute come lo strumento ricettivo delle regole e degli obblighi individuati e di seguito strutturati rispetto allo specifico core di per il quale nasce l'esigenza di trasferire dati all'estero.

Le BCR dovranno assolutamente perimetrare l'ambito geografico e materiale del documento, delimitandone i limiti territoriali di applicabilità nonché i limiti oggettivi legati al trasferimento (rectius trattamento): dati relativi al personale dipendente, ai clienti, ai fornitori ecc.

Occorre porre attenzione nella scrittura delle BCR alla richiesta fondamentale di registrare per esse una puntuale e adeguata trasposizione dei "principi guida" previsti dalla normativa ai trattamenti dei dati personali, facendo cosi nascere l'obbligatoria menzione delle finalità che si vogliano perseguire non solo mediante il trasferimento, ma anche attraverso il trattamento generale delle suddette informazioni, il tutto sempre all'interno del principio di proporzionalità e di necessità che congiuntamente valutano e proteggono l'intero flusso di informazioni.

Nella costruzione e comunque nell'impianto per la definizione di una BCR non dovranno mancare, anzi dovranno essere ben chiare ed esplicitate, le basi legali che legittimano ogni trattamento del dato personale, ovvero il consenso dell'interessato o in alternativa la dove previsto rappresentano una delle condizioni di esonero così come sancite dall'articolo 7 della Direttiva, o in alternativa essere di fronte ad un trattamento necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di quest'ultima o ancora si sia di fronte ad un trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare.

Con riferimento agli strumenti che si dovranno implementare, ci si ricordi che si dovrà garantire

- 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.

Adempimenti

Il trasferimento di dati personali, soprattutto se si trasferiscono dati sensibili[1], come ogni trattamento, deve essere innanzitutto conforme alle disposizioni generali in materia di protezione dei dati personali, in relazione alle finalità per cui viene effettuato, quindi deve essere:

- fondato su una base giuridica tra quelle previste all'art. 6 del GDPR;
- eseguito nel pieno rispetto dei princìpi elencati all'art.5 del GDPR e, in generale, di tutte le altre normative applicabili ai trattamenti di dati personali;
- inserito nel Registro dei trattamenti, riportando i paesi terzi o le organizzazioni internazionali a cui i dati personali sono stati o saranno comunicati, la valutazione del rischio effettuata e la descrizione delle garanzie attuate per il trasferimento, in relazione ai rischi valutati (ciò affinché l'interessato benefici di un adeguato livello di protezione dei suoi dati personali sia nel trasferimento dei dati verso un paese terzo sia nell'eventuale ulteriore trasferimento da questi ad altro paese terzo, secondo le disposizioni del Capo V del GDPR);
- inserito nell'informativa per l'interessato, riportando quali sono i paesi terzi o organizzazioni internazionali destinatarie e le motivazioni per cui ha luogo il trasferimento; devono essere inoltre riportate le valutazioni del Titolare in merito alla scelta dello strumento di garanzia adottato, tra quelli previsti dal GDPR, in caso di assenza di una decisione di adeguatezza.

La valutazione dell'adeguatezza della tutela offerta da un paese terzo va considerata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti, che riguardano anche la modalità, la frequenza, la durata e il contesto del trasferimento.

Sia nella valutazione del rischio sia nelle garanzie attuabili, Sapienza presta attenzione anche ai trasferimenti che potrebbero subentrare tra l'importatore dei dati e un successivo sub-incaricato, in virtù di un subcontratto dell'importatore.

[1] Fra i più importanti provvedimenti del Garante della Privacy circa il trattamento dei dati "sensibili" vedi: - Autorizzazione generale n. 1/2016 al trattamento dei dati sensibili nei rapporti di lavoro 15 dicembre 2016; Autorizzazione generale n. 2/2016 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale 15 dicembre 2016; Autorizzazione generale n. 3/2016 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni;15 dicembre 2016 Autorizzazione generale n. 4/2016 al trattamento dei dati sensibili da parte dei liberi professionisti 15 dicembre 2016; - Autorizzazione generale n. 5/2016 al trattamento dei dati sensibili da parte di diverse categorie di titolari 15 dicembre 2016; Autorizzazione generale n. 6/2016 al trattamento dei dati sensibili da parte degli investigatori privati 15 dicembre 2016; Autorizzazione generale n. 7/2016 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici;15 dicembre 2016; - Autorizzazione generale n. 8/2016 al trattamento dei dati genetici 15 dicembre 2016; Autorizzazione generale n. 9/2016 al trattamento dei dati personali effettuato per scopi di ricerca scientifica 15 dicembre 2016.

La roadmap per il trasferimento sicuro: i sei step

Come primo passo, l'EDPB[2] consiglia di verificare compiutamente il numero di trattamenti che prevedono un trasferimento di dati personali all'estero, nonché di censire i soggetti coinvolti in detto trasferimento. Non solo: occorre verificare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione agli scopi per i quali sono trasferiti e trattati nel Paese terzo.

Il secondo passo consiste invece nella verifica sulla sussistenza di uno degli strumenti idonei al trasferimento, tra quelli indicati agli artt. 44 ss. del GDPR.

Se in caso di ricorrenza di una decisione di adeguatezza della Commissione non è necessario adottare ulteriori misure, nel caso di adozione di clausole standard (SCC), norme vincolanti di impresa (BCR), codici di condotta, meccanismi di certificazione e clausole contrattuali ad hoc, potrebbe verificarsi che la situazione del Paese terzo importatore (o meglio la sua legislazione) richieda di integrare questi strumenti di trasferimento con misure supplementari per garantire un livello di protezione sostanzialmente equivalente.

Il riferimento del Comitato va alle leggi che stabiliscono i requisiti per la disclosure di dati personali alle autorità pubbliche o che conferiscono a tali autorità pubbliche poteri di accesso ai dati personali (ad esempio per l'applicazione del diritto penale, il controllo regolamentare e la sicurezza nazionale): l'esercizio di tali poteri dovrà risultare limitato a quanto necessario e proporzionato in una società democratica per rendere effettiva la garanzia per il trasferimento.

Laddove il livello di protezione non possa dirsi equivalente a quello garantito dall'Unione, a fronte dell'impedimento per l'importatore costituito dalla legislazione e/o dalle pratiche del Paese terzo applicabile al trasferimento, occorrerà mettere in atto misure supplementari efficaci preliminarmente al trasferimento dei dati personali (questa valutazione costituisce il terzo step).

Il quarto passo consiste quindi nell'individuare e adottare le misure supplementari necessarie per portare il livello di protezione dei dati trasferiti allo standard di equivalenza essenziale dell'UE.

In linea di principio, le misure supplementari possono avere carattere contrattuale, tecnico o organizzativo: in alcuni scenari, infatti, solo misure tecniche potrebbero ostacolare o rendere inefficace l'accesso ai dati personali da parte delle autorità pubbliche, nelle circostanze in cui tale accesso risulti al di là di quanto necessario e proporzionato in una società democratica.

Le ultime due fasi sono costituite dalle necessarie autorizzazioni che potrebbero essere richieste dallo strumento di trasferimento prescelto e dall'attività di verifica ed aggiornamento.

[2] Comitato europeo per la protezione dei dati

Condizioni per la legittimità del trasferimento

I dati possono essere trasferiti solo in presenza di almeno una delle seguenti condizioni, ovvero una delle relative sotto-casistiche, che saranno dettagliate nei successivi paragrafi:

1. **Decisione di adeguatezza**: se la Commissione Europea ha deciso che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale in questione, garantiscono un livello di protezione dei Dati Personali adeguato il trasferimento è possibile senza altre autorizzazioni specifiche.
2. **Garanzie adeguate**: qualora non vi sia una decisione di adeguatezza, il trasferimento può essere effettuato in presenza di garanzie adeguate e in forza di condizioni per le quali gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Esse sono costituite alternativamente da:
   a. uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
   b. norme vincolanti d'impresa (BCR) in conformità dell'art. 47 GDPR;
   c. clausole contrattuali tipo o standard di protezione dei dati, adottate dalla Commissione Europea secondo la procedura d'esame di cui all'art. 93, par. 2) GDPR;
   d. clausole contrattuali tipo o standard di protezione dei dati, adottate da un'Autorità di Controllo e approvate dalla Comm. Europea secondo la procedura d'esame di cui all'art. 93, par. 2) GDPR;
   e. un Codice di Condotta (CC) approvato a norma dell'art. 40 GDPR, unitamente all'impegno vincolante ed esecutivo da parte del Titolare del trattamento o del Responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
   f. un Meccanismo di Certificazione (MC) approvato a norma dell'art. 42 GDPR, unitamente all'impegno vincolante ed esigibile da parte del Titolare del trattamento o del Responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
   g. Clausole Contrattuali tra il Titolare del trattamento o il Responsabile/Designato del trattamento e il Titolare del trattamento, il Responsabile del trattamento o il destinatario dei Dati Personali nel Paese terzo o nell'organizzazione internazionale (con l'autorizzazione dell'Autorità di Controllo competente);
   h. disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli Interessati (con l'autorizzazione dell'Autorità di Controllo competente);
   i. autorizzazioni rilasciate da uno Stato membro o dal GDPD in base alla precedente direttiva 95/46/CE, che restano valide fino a quando non vengono modificate, sostituite o revocate dalla medesima autorità di controllo (art. 46.5).
3. **Deroghe in specifiche situazioni**: in mancanza di una delle precedenti condizioni di legittimità, è possibile trasferire i Dati Personali solo se si verifica una delle seguenti situazioni vincolanti (da considerare residuali nel loro utilizzo rispetto a quelle riportate in precedenza) e che, per il loro utilizzo da parte di Sapienza o di una Pubblica amministrazione, richiedono la concomitante presenza di altri fattori, come nel seguito schematizzato. Le condizioni sono, in alternativa:
   a. che l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
   b. che il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il

Titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c. che il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare del trattamento e un'altra persona fisica o giuridica a favore dell'Interessato;
d. che il trasferimento sia necessario per importanti motivi di interesse pubblico;
e. che il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f. che il trasferimento sia necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora essi si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
g. che il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri;
h. se non è ripetitivo, se riguarda un numero limitato di interessati, se è necessario per il perseguimento degli interessi legittimi cogenti del Titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'Interessato;

Ad esse si aggiunge la condizione prevista all'art. 28, paragrafo 3.a), per la quale il Responsabile/Designato del trattamento può effettuare il trasferimento dei dati verso un paese estero, pur non avendolo tra le istruzioni del Titolare, quando lo prevede il diritto dell'UE o dello Stato membro cui è soggetto. In tal caso ne informa il Titolare, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

Decisione di adeguatezza

La novità del GDPR riguarda la possibilità che la decisione di adeguatezza della CE possa essere adottata anche su un territorio o uno o più settori specifici all'interno di un paese estero e non necessariamente sull'interezza di questo. Ulteriore elemento di novità è la possibilità che la decisione possa essere revocata tramite un meccanismo di riesame periodico - almeno ogni 4 anni - tenendo conto degli sviluppi che in tali paesi potrebbero incidere sul funzionamento delle decisioni già adottate.

La Commissione deve, difatti, valutare l'adeguatezza di un paese per un trasferimento di dati personali, tenendo conto innanzitutto dello stato di diritto e del rispetto dei diritti umani e delle libertà fondamentali, della pertinente legislazione generale e settoriale, anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale, accesso delle autorità pubbliche ai dati personali e norme inerenti il trasferimento successivo dei dati personali verso un altro paese estero, osservate nel paese terzo o organizzazione internazionale.

Il concetto di adeguatezza è finalizzato anche ad escludere il ricorso a trattamenti in paesi terzi diretti ad eludere la normativa UE, richiedendo che le misure adottate nel paese terzo o organizzazione internazionale siano basate sui medesimi princìpi Ue di protezione dei dati e dimostrino un'efficacia verificabile: il che dovrà includere la presenza di un impianto sanzionatorio adeguato per la loro eventuale violazione e la disponibilità per l'interessato di diritti azionabili e mezzi di ricorso effettivi, in sede amministrativa e giudiziaria, quali quelli garantiti nell'ambito territoriale di applicazione del GDPR.

Sono considerate equiparate a tali decisioni quelle adottate dalla Commissione in base all'art. 25 paragrafo 6 della direttiva 95/46/CE e che continuano ad essere valide fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata mediante atti di

esecuzione, al pari delle decisioni adottate sulla base del GDPR. Difatti esse venivano assunte sulla base di una procedura di valutazione, fondata sul parere di un comitato di supporto alla Commissione prevista all'art. 31 paragrafo 2 della stessa direttiva, con una procedura assimilabile a quella attualmente prevista per gli atti di esecuzione.

Tutte le decisioni sono pubblicate sul sito della Commissione (e anche del Garante).

Approfondimenti sulle Garanzie adeguate

Secondo il principio della non tassatività e in linea con l'accountability del Titolare, in assenza di decisioni di adeguatezza è possibile ricorrere a garanzie adeguate, descritte all'art. 46 e precedentemente riportate, in alcuni casi con la necessità di autorizzazione specifica da parte di un'Autorità di controllo.

Le garanzie previste all'art. 46 mirano a rendere disponibili agli Interessati diritti azionabili e mezzi di ricorso effettivi. Tra queste, come si è accennato, continuano a rimanere valide le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'art. 26, paragrafo 2 della direttiva 95/46/CE fino a quando non vengano modificate, sostituite o abrogate dalla medesima autorità di controllo.

Continuano pertanto ad essere valide le autorizzazioni nazionali emesse dal Garante, anche in conseguenza di decisioni di adeguatezza della Commissione adottate sulla precedente normativa, riportate sulle pagine del Garante.

Si noti bene che le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo, che dispongano il trasferimento di dati personali da parte di un Titolare o Responsabile del trattamento, possono essere riconosciute o assumere un carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, fatti salvi gli altri presupposti al trasferimento di cui al capo V del GDPR (art. 48 e considerando 115). E' questo il caso, ad esempio, dell'Accordo tra Unione europea e Stati Uniti in materia di estradizione del 25 giugno 2015 e di altri accordi presenti sulla pagina del Ministero della giustizia – Atti internazionali. Questo perché la presenza di un accordo internazionale (o anche di mutua collaborazione giudiziaria) in vigore tra lo Stato membro e il paese terzo fornisce una garanzia, da parte di questi, di tutela dei principi, dei diritti e delle libertà fondamentali dell'UE; diversamente, la mera applicazione extraterritoriale di leggi, regolamenti e atti normativi del paese terzo potrebbe creare una situazione contraria al diritto della protezione dati.

Rivedendo l'elenco delle garanzie adeguate, si può aggiungere che:

a) strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici: per avere validità, gli accordi internazionali stipulati tra soggetti pubblici europei e dei paesi esteri non devono incidere sul diritto dell'UE o sul GDPR, ossia contraddirlo o limitarne la portata. Inoltre devono essere conclusi da autorità pubbliche o organismi pubblici, devono essere giuridicamente vincolanti ed avere efficacia esecutiva sia nel paese terzo sia nei territori dell'UE;

b) norme vincolanti d'impresa (BCR): requisito fondamentale per attingere a tale strumento è l'appartenenza della società "importatrice" ed "esportatrice" al medesimo gruppo societario (anche se situate in due paesi diversi). Non sono pertanto applicabili in ambito universitario;

c) clausole contrattuali tipo: sono testi contrattuali standard sottoscritti da ambo le parti, solitamente allegati ai contratti di servizio. Esistono:

   i) clausole tipo della Commissione Europea[3]: le più recenti sono state approvate dalla Commissione a febbraio 2010 e sono considerate ancora valide in base all'art.46.5 e il C106;

   ii) clausole tipo adottate dalla DPA nazionale (novità): esse possono essere comunicate come "decisione di adozione" da parte del GDPD al Comitato per la protezione dati Comitato Europeo per la Protezione dei Dati (European Data Protection Board - EDPB), secondo l' art. 64.1.d, e approvate dalla Commissione europea secondo atti d'esecuzione, al fine di garantire un'omogenea applicazione della normativa all'interno di ciascuno stato membro e

[3] Sono di due tipi: una per trasferimenti da un Titolare ad un Titolare fuori UE, l'altra per trasferimenti da un Titolare ad un responsabile fuori UE1

dell'UE;

iii) clausole contrattuali ad hoc tra le parti: questa condizione di garanzia esplicita un requisito precedentemente più vago e, nel caso in cui le model clause siano stipulate tra il Titolare o responsabile (esportatore) e l'importatore (altro Titolare o responsabile extra UE), impone che tali contratti, anche di natura privata, siano sottoposti al GDPD. Questi ha il compito di autorizzarne la validità (art. 58 paragrafo 3.h) e di comunicare tale decisione al Comitato2 perché possa emettere un parere, secondo il principio di coerenza di cui all'art.63;

Le clausole-tipo di protezione dati non ammettono emendamenti e devono essere sottoscritte dalle parti. Solitamente riguardano solo gli aspetti inerenti la protezione dei dati3, pertanto vengono incorporate in un contratto più generale di Data Transfer e vi si possono aggiungere clausole ulteriori purché non in conflitto, direttamente o indirettamente, con quanto approvato dalla Commissione europea;

d) contratto di diritto amministrativo tra autorità o organismi pubblici: sono considerate garanzie adeguate le disposizioni inserite in accordi amministrativi tra tali soggetti pubblici se comprendono diritti effettivi e azionabili per gli interessati. Un esempio può essere rappresentato dal Memorandum d'intesa che, pur non essendo un vero e proprio contratto, è un documento giuridico che esprime una convergenza di interessi fra le parti, indicando una comune linea di azione prestabilita e comune per i diritti effettivi ed azionabili degli interessati. Sempre per il principio di coerenza, anche in questo caso va subordinato ad autorizzazione del GDPD (art. 58 paragrafo 3.i) e deve seguire l'iter indicato al punto c.iii).

Da notare che l'ultimo capoverso del Considerando 109 invita i Titolari del Trattamento e i Responsabili del Trattamento a fornire garanzie supplementari attraverso impegni contrattuali che integrino le Clausole tipo di protezione dati. Allo stesso modo, i Codici di condotta (art. 40) e i Meccanismi di Certificazione (art. 42) costituiscono strumenti validi se accompagnati da un impegno vincolante ed esecutivo, assunto dalla parte stabilita nel paese extra UE, ad attuare garanzie adeguate rispetto ai principi di protezione dati, che prevedano sanzioni e meccanismi di esercizio dei diritti da parte degli interessati.

Trasferimento effettuato in base a deroghe

Deroghe e necessità

Scopo del GDPR è garantire agli interessati la disponibilità di diritti azionabili e mezzi di ricorso effettivi attraverso una serie di strumenti giuridici tipici per cui è consentito ricorrere al meccanismo delle deroghe, previste all'art. 49, solo eccezionalmente.

I trasferimenti fondati su una deroga non necessitano di alcuna autorizzazione preventiva del GDPD e presentano quindi rischi maggiori per i diritti e le libertà degli interessati; devono quindi essere interpretate in maniera restrittiva, rimanere un'eccezione e non una regola nei trasferimenti del Titolare.

Quando i trasferimenti avvengono nell'ambito della normale attività o prassi commerciale, devono essere messe in atto garanzie adeguate ai sensi dell'art. 46 piuttosto che ricorrere alle deroghe.

Con le Linee guida 2/2018 l'EDPB, basandosi sul documento WP 114 del gruppo WP29, ha fornito una serie di orientamenti per l'applicazione del meccanismo delle deroghe ai trasferimenti verso paesi terzi o organizzazioni internazionali, tenendo conto del Considerando 111 e ponendo, come presupposto di fondo per il ricorso alle deroghe, la "necessità" del trasferimento dei dati per una determinata finalità.

Test di necessità

Le deroghe di cui all'art. 49, paragrafo 1 lettere da b) a f), prevedono che "il trasferimento sia necessario...". Tale condizione deve essere verificata mediante un test di necessità da parte del Titolare, volto ad evidenziare il nesso stretto e specifico tra i dati personali oggetto del trasferimento e le finalità del trattamento della specifica deroga che ritiene di applicare. Il trasferimento può avvenire solo se le finalità sono necessarie, concrete e non presunte, o possibili, e i dati strettamente pertinenti e necessari allo scopo.

Quali rischi

Il gruppo di lavoro della Commissione Europea, già nel 19984, riteneva che fra le categorie di trasferimenti che rappresentano una minaccia particolare per la vita privata e meritano quindi particolare attenzione siano comprese le seguenti:

- trasferimenti riguardanti le categorie particolari di dati;
- trasferimenti che comportano rischi di perdite finanziarie (ad esempio pagamenti con carta di credito attraverso Internet);
- trasferimenti che comportano rischi per la sicurezza personale;
- trasferimenti finalizzati all'adozione di una decisione particolarmente importante per la persona interessata (assunzioni, promozioni, concessione di un credito, ecc.);
- trasferimenti che rischiano di causare un grave imbarazzo a una persona o di lederne la reputazione;
- trasferimenti che possono condurre ad azioni specifiche che costituiscono un'ingerenza grave nella vita privata della persona;
- trasferimenti ripetuti che riguardano grandi volumi di dati (per es. dati su transazioni elaborati su reti di telecomunicazioni, Internet, ecc.);
- trasferimenti che comportano la raccolta di dati per mezzo di nuove tecnologie secondo modalità particolarmente occulte o clandestine (per es. i cosiddetti "cookies" di Internet), cui potrebbe oggi aggiungersi l'utilizzo diffuso di servizi in cloud anche per la gestione dei dati dei lavoratori o per lo scambio di dati per attività di lavoro e ricerca.

I rischi per i diritti e le libertà delle persone fisiche, di cui tenere conto, sono ulteriormente elencati

ai considerando 75 e 76 del GDPR.

Matrice di applicazione delle deroghe

Di seguito viene riportata una schematizzazione delle condizioni di applicazione delle deroghe di cui al paragrafo 1 art. 49 del GDPR che, sono da considerare residuali nel loro utilizzo, sottolineando che anche le deroghe non espressamente limitate ai trasferimenti "occasionali" e "non ripetitivi" devono essere interpretate come eccezionali rispetto alla regola.

Condizioni per il trasferimento condizione a)

E' condizione necessaria che l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'Interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate.

Eccezioni per la PA condizione a)

Non applicabile nell'esercizio di pubblici poteri (art. 49.3)

Gestione Informativa Consenso o al Registro dei trattamenti condizione a)

Il consenso è visto e scritto come base giuridica, che deve essere esplicito, informato e specifico, indicando i paesi di destinazione, i destinatari o le categorie di destinatari, i possibili rischi derivanti dall'assenza, nel paese terzo, di un'autorità di controllo e la possibilità che non siano previsti principi di legittimità del trattamento e diritti per l'interessato mancando un parere di adeguatezza

Attenzioni e riferimenti condizione a)

Sussistendo sempre la possibilità della la revoca in qualsiasi momento non è utilizzabile per trasferimenti di lungo periodo. Il consenso deve essere esplicito, dopo minuziosa informazione dei possibili rischi, e nel pieno rispetto delle condizioni agli artt. 4.11, 7, 13 e 14, dei C32, C33, C42 e C44 GDPR e delle linee guida sul consenso WP259 del WP29. La specificità impone che il consenso valga solo per quel trasferimento specifico di cui è informato e le circostanze del trasferimento non siano modificate dopo la prestazione del consenso.

Condizioni per il trasferimento condizione b)

E' condizione basilare che il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il Titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato.

Eccezioni per la PA condizione b)

Non applicabile nell'esercizio di pubblici poteri (art. 49.3), in questa casistica è prevista l'applicazione per trasferimenti occasionali

Gestione Informativa Consenso o al Registro dei trattamenti condizione b)

Nell'informativa o quanto meno a seguire nel consenso deve essere chiara l'occasionalità del trasferimento e quale sia il nesso stretto e significativo tra il trasferimento dei dati, i dati trasferiti e le finalità del contratto.

Attenzioni e riferimenti condizione b)

Quanto detto in questa casistica risulta non utilizzabile per trasferimenti di dati aggiuntivi, non strettamente necessari per l'esecuzione del contratto o delle misure precontrattuali. Nel caso di trasferimenti ripetuti devono essere utilizzate le misure di garanzie art. 46.

Condizioni per il trasferimento condizione c)

Che il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare del trattamento e un'altra persona fisica o giuridica a favore dell'Interessato

Eccezioni per la PA condizione c)

Non applicabile nell'esercizio di pubblici poteri (art. 49.3), in questa casistica è prevista l'applicazione per trasferimenti occasionali

Gestione Informativa Consenso o al Registro dei trattamenti condizione c)

Nell'informativa o quanto meno a seguire nel consenso deve essere chiara l'occasionalità del trasferimento e quale sia il nesso stretto e significativo tra il trasferimento dei dati, i dati trasferiti e le finalità del contratto.

Attenzioni e riferimenti condizione c)

Quanto detto in questa casistica risulta non utilizzabile per trasferimenti di dati aggiuntivi, non strettamente necessari per l'esecuzione del contratto o delle misure precontrattuali. Nel caso di trasferimenti ripetuti devono essere utilizzate le misure di garanzie art. 46.

Condizioni per il trasferimento condizione d)

Trasferimento necessario per importanti motivi di interesse pubblico

Eccezioni per la PA condizione d)

Caso di richieste da paesi terzi (art. 48)

Gestione Informativa Consenso o al Registro dei trattamenti condizione d)

Vista l'eccezionalità e si ritiene l'urgenza o il principio pubblico non vi sono attività da fare nel merito.

Attenzioni e riferimenti condizione d)

In continuità con l'art. 26.1.d della direttiva 95/46/CE il trasferimento può avvenire solo qualora sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, deducibile dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, anche in virtù della reciprocità per la cooperazione internazionale sottoscritta tramite accordo o convenzione internazionale. Nel wp114 del 25 novembre 2015 il WP29 afferma che "questa deroga può essere utilizzata solo se il trasferimento è nell'interesse delle autorità stesse di uno Stato membro dell'Ue e non unicamente nell'interesse di una o più autorità di un paese terzo".

Il requisito essenziale è nell'indicazione di un interesse pubblico, non nella natura dell'organizzazione che trasferisce o riceve i dati, che può essere anche privata (C111, C112)..

Condizioni per il trasferimento condizione e)

che il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

Eccezioni per la PA condizione e)

Naturalmente in questi casi non si prevede nessuna eccezione e il trasferimento può essere anche occasionale

Gestione Informativa Consenso o al Registro dei trattamenti condizione e)

Vista l'eccezionalità e si ritiene l'urgenza o il principio pubblico non vi sono attività da fare nel merito.

Attenzioni e riferimenti condizione e)

Poiché il trasferimento deve essere effettuato nell'ambito del procedimento, è necessario un nesso stretto tra i dati trasferiti e il procedimento specifico relativo alla situazione in questione. I procedimenti devono avere un fondamento giuridico e possono includere la fase preprocessuale, l'apertura di un contenzioso o la richiesta di approvazione di una fusione. Nel diritto nazionale di alcuni Stati esistono i "blocking statutes" che impediscono o limitano i trasferimenti di dati personali verso autorità giudiziarie o talvolta organismi pubblici di paesi terzi. Occorrerebbe prima verificare se possano essere utilizzati dati anonimi

o pseudonimizzati[4].

Condizioni per il trasferimento condizione f)

Che il trasferimento sia necessario per tutelare gli interessi dell'Interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso.

Eccezioni per la PA condizione f)

Naturalmente in questi casi la deroga è valida solo quando l'interessato è nell'incapacità fisica o giuridica di prestare il consenso

Gestione Informativa Consenso o al Registro dei trattamenti condizione f)

Non vi sono attività specifiche da fare nel merito.

Attenzioni e riferimenti condizione f)

Nei casi in cui c'è capacità decisionale ed è possibile dare il consenso la deroga non è applicabile.

Il trasferimento deve essere correlato all'interesse individuale dell'interessato o di un'altra persona e, nel caso di dati sanitari, deve essere necessario ai fini di una diagnosi essenziale. E' esclusa la ricerca medica che produrrà risultati solo in futuro.

Il grave rischio imminente deve essere superiore rispetto le preoccupazioni connesse alla protezione

Condizioni per il trasferimento condizione g)

Che il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

Eccezioni per la PA condizione g)

Non vi sono eccezioni dichiarate

Gestione Informativa Consenso o al Registro dei trattamenti condizione g)

Non vi sono attività specifiche da fare nel merito.

Attenzioni e riferimenti condizione g)

La deroga si applica a dati contenuti in registri aventi la finalità di trasmettere informazioni al pubblico, non ai registri privati. Si tratta di registri che possono essere consultati dal pubblico, in generale, o da chiunque sia in grado di dimostrare un legittimo interesse (registri delle imprese, di condanne penali o casellario giudiziale, registri catastali, pubblici registri automobilistici….). **Non può riguardare la totalità dei dati né intere categorie di dati personali contenuti nel registro**. Se il registro è costituito per legge per essere consultato da persone che hanno un legittimo interesse, il trasferimento può avvenire su loro richiesta o se ne sono destinatarie (quindi non tramite pubblicazione erga omnes), tenendo conto degli interessi e dei diritti fondamentali dell'interessato. 1

Condizioni per il trasferimento condizione h)

Il trasferimento se non è ripetitivo, se riguarda un numero limitato di interessati, se è necessario per il perseguimento degli interessi legittimi cogenti del Titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'Interessato; il Titolare del trattamento deve aver valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei Dati Personali. Il Titolare del trattamento informa del trasferimento l'Autorità di Controllo. In aggiunta alla fornitura di informazioni di cui agli artt. 13 e 14 GDPR, il Titolare del trattamento informa l'Interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

4 La pseudonimizzazione è una tecnica che consiste "nel trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (art. 4 punto 5 del GDPR).

Eccezioni per la PA condizione h)

Non utilizzabile nell'esercizio di pubblici poteri (art.49.3) (condizione dal secondo capoverso lett. g). condizione applicabile anche per trasferimenti eccezionali

Gestione Informativa Consenso o al Registro dei trattamenti condizione h)

Il Titolare deve informare l'interessato. Vanno descritti i legittimi interessi cogenti e i seri motivi per i quali non è stato possibile tutelare il trasferimento con garanzie adeguate o alcuna delle altre deroghe previste, inserendo i paesi destinatari.

Devono essere indicate nel Registro dei trattamenti sia la valutazione delle circostanze relative al trasferimento sia le garanzie adeguate fornite a seguito della valutazione..

Attenzioni e riferimenti condizione h)

E' prevista come extrema ratio, applicabile solo nel caso in cui non è possibile basare il trasferimento su una disposizione art. 45 o 46 né su alcuna delle deroghe sopra elencate; ai sensi del C113, deve riguardare un numero limitato di interessati ed è subordinato alla concomitante sussistenza delle condizioni espressamente elencate nell'intero capoverso riportato dopo la lettera g) paragrafo 1 art.49.

L'interesse legittimo deve essere cogente poiché non vi rientrano tutti i possibili interessi di cui all'art.6, paragrafo 1.f); deve esserne informato il GDPD.

Il paragrafo 5 dell'art.49 del GDPR pone una deroga alle deroghe, lasciando possibilità all'Unione o agli Stati membri, in assenza di una decisione di adeguatezza, di fissare limiti al trasferimento di categorie specifiche di dati verso paesi esteri per importanti motivi di interesse pubblico, notificandolo alla Commissione.

Brexit

Dal 12 febbraio 2019 è stata diffusa una nota dell'EDPB con la quale si informa che, in assenza di un accordo fra i Paesi dello Spazio Economico Europeo (ossia UE + Norvegia, Liechtenstein, Islanda) e il Regno Unito, questi diverrà un Paese terzo. Conseguentemente, il trasferimento di dati personali verso il Regno Unito dovrà basarsi su uno degli strumenti giuridici finora indicati e secondo l'ordine di garanzia preferibile e riportato:

- clausole-tipo di protezione dati o clausole ad-hoc;
- norme vincolanti d'impresa;
- codici di condotta e meccanismi di certificazione;
- deroghe.

Nella stessa comunicazione si consiglia di iniziare a provvedere a 5 step di adeguamento a tale situazione, consistenti nell'individuare tra i trattamenti effettuati quali siano quelli che richiedono trasferimenti di dati verso il Regno Unito, individuare quali tra gli strumenti prima elencati possa essere applicato, implementare tale strumento provvedendo ad aggiornare i documenti interni (p.e. Registro dei trattamenti) e modificare le informative.

Sanzioni

Le sanzioni amministrative per le violazioni degli artt. da 44 a 49 sono previste all'art.83, comma 5 lett. c) e comportano, fatti salvi i principi di proporzionalità, importi fino a 20.000.000 di Euro e da uno a tre anni di reclusione in base all'art.167 comma 3 del D. Lgs.196/2003.

Riferimenti

Art. 167 Nuovo Codice Privacy – D.lgs 196/2003 aggiornato al D.lgs 101/2018

Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.
2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septiesovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.
3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sè o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attivita' di accertamento delle violazioni delle disposizioni di cui al presente decreto.
6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

Articolo 47 - Norme vincolanti d'impresa

1. L'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63, a condizione che queste:

a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;

b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali; e

c) soddisfino i requisiti di cui al paragrafo 2.

2. Le norme vincolanti d'impresa di cui al paragrafo 1 specificano almeno:

a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;

b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;

c) la loro natura giuridicamente vincolante, a livello sia interno che esterno;

d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;

e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;

f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;

g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14;

h) i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 37 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami; (1)

i) le procedure di reclamo;

j) i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;

k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;

l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);

m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è

soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e

n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

3. La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa ai sensi del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Articolo 48 -Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

Considerando 113

Potrebbero altresì essere autorizzati i trasferimenti qualificabili come non ripetitivi e riguardanti soltanto un numero limitato di interessati ai fini del perseguimento degli interessi legittimi cogenti del titolare del trattamento, a meno che non prevalgano gli interessi o i diritti e le libertà dell'interessato e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento. Il titolare del trattamento dovrebbe considerare con particolare attenzione la natura dei dati personali, la finalità e la durata del trattamento o dei trattamenti proposti, nonché la situazione nel paese d'origine, nel paese terzo e nel paese di destinazione finale, e dovrebbe offrire garanzie adeguate per la tutela dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali. Tali trasferimenti dovrebbero essere ammessi soltanto nei casi residui in cui nessuno degli altri presupposti per il trasferimento è applicabile. Per finalità di ricerca scientifica o storica o a fini statistici, è opportuno tener conto delle legittime aspettative della società nei confronti di un miglioramento delle conoscenze. Il titolare del trattamento dovrebbe informare l'autorità di controllo e l'interessato in merito al trasferimento.

Considerando 115

Alcuni paesi terzi adottano leggi, regolamenti e altri atti normativi finalizzati a disciplinare direttamente le attività di trattamento di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. Essi possono includere le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento e non sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria. L'applicazione extraterritoriale di tali leggi, regolamenti e altri atti normativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della protezione delle persone fisiche assicurata nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale, tra l'altro, quando la comunicazione è necessaria per un rilevante motivo di interesse pubblico riconosciuto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento.