

Autore/Entità:
Responsabile di LP/UOT, Direttori Servizi Gruppo
Data: XX/XX/2008
Classificazione: D3

Allegato 4

Memorandum della Direttiva
Protezione e trasferimento dei dati personali
al di fuori dell'Unione Europea

1 - Indicazioni per il Management

Perchè ci servono le Norme Vincolanti d'Impresa e una Direttiva Gruppo?

Le Norme Vincolanti d'Impresa servono a regolare il trasferimento di dati personali all'interno del Gruppo ed a garantire che, così come richiesto dalla legislazione UE, le persone i cui dati personali sono protetti in Europa continuino a beneficiare di tale protezione quando i loro dati lasciano il territorio Europeo per esser trattati al di fuori della UE, in paesi che non offrono un adeguato livello di protezione. La Direttiva Gruppo fa sì che le regole in essa contenute siano applicabili a tutte le entità del Gruppo.

Perchè adesso?

Il numero di situazioni in cui i trasferimenti internazionali di dati avvengono sta aumentando, per esempio la centralizzazione delle basi dati all'interno del Gruppo. Poichè i trasferimenti di dati possono essere numerosi e svariati, l'adozione delle Norme Vincolanti d'Impresa evita di stipulare un nuovo contratto per ciascun trasferimento. Le regole assicurano anche che il trattamento garantisca una protezione adeguata della riservatezza e dei diritti umani, in particolare all'interno delle Società del Gruppo situate in paesi al di fuori dell'Unione Europea che non forniscono adeguati livelli di protezione.

2 – Indicazioni sullo studio di fattibilità

Disposizioni per l'attuazione della Direttiva

Per facilitare l'applicazione delle regolamentazioni nazionali e delle Norme Vincolanti d'Impresa sul trasferimento dei dati personali al di fuori dell'Unione Europea, verrà definita una struttura per includere i Privacy Officer designati all'interno dei Servizi Giuridici di Michelin.

I Privacy Officers avranno il compito di garantire:

1. il rispetto della legge nel loro paese
2. l'applicazione delle Norme Vincolanti d'Impresa in ciascun paese al di fuori dell'Unione Europea. Ciò evidentemente nel presupposto che le norme sulla protezione dei dati si applichino in paesi che forniscono un adeguato livello di protezione.

Questo copre un rischio rilevante?

Il trasferimento di dati da parte di un'Entità europea che non aderisce alle condizioni stabilite dalle leggi di protezione nel relativo paese sarà illegale e potrà come tale implicare la responsabilità della persona che effettua il trattamento.

Quali risorse sono disponibili?

Le risorse disponibili sono basate sull'organizzazione e sul ruolo chiave dei Privacy Officer che saranno responsabili della promozione della cultura della Protezione dei Dati così come le Interfacce in ciascun settore di ogni entità. I ruoli che i Privacy Officer devono coprire sono chiaramente definiti così come i loro obiettivi annuali.

3 - Implementazione

3.1 Principi di base

Questi principi sono stabiliti nella Direttiva Gruppo. Le Entità Europee e non Europee del Gruppo che non forniscono un adeguato livello di protezione hanno obblighi a cui debbono attenersi quando trattano dati personali che sono o sono stati trasferiti.

3.2 Metodologia:

Una metodologia che farà parte “della politica di responsabilità e performance”

4 - Verifica e migliorie all'attuazione

I Privacy Officer garantiranno ogni anno due revisioni per accertare l'attuazione e/o identificare tutte le difficoltà incontrate. Queste revisioni saranno trasmesse al Comitato per la Protezione dei Dati Personali.