PRIVACY
(Regolamento Europeo 679/2016 - operativo dal 25 maggio 2018)

Nota sulle Linee Guida concernenti la valutazione di impatto sulla protezione dei dati (DPIA)

Commento alle Linee Guida sulla DPIA

Le Linee Guida redatte dal Gruppo di lavoro articolo 29 (o Working Party art. 29, di seguito **WP29**)[1] offrono degli interessanti spunti per l'applicazione del nuovo **Regolamento generale per la protezione dei dati personali** (General Data Protection Regulation o **GDPR)** e per garantire una corretta *compliance* al medesimo.

La valutazione di impatto dei rischi nel trattamento dei dati, ***Data Protection Impact Assessment*** (**DPIA**), consiste in una **procedura** che il titolare del trattamento dati deve mettere a punto per **descrivere** il trattamento che effettua, valutarne la necessità e la proporzionalità, nonché per facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche coinvolte.[2]

In particolare, il WP29, nell'elaborazione delle Linee Guida distingue tra la valutazione di impatto come ***analisi*** dei trattamenti dei dati (esposti a rischi) e la valutazione di impatto come ***individuazione delle misure*** specifiche da adottarsi per i trattamenti per i quali la verifica effettuata richiede particolari cautele.

Non è obbligatorio procedere ad una DPIA se non in presenza di condizioni particolari e cioè ***ogni qual volta il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche*.**

[1] Il WorkingParty29_Gruppo di lavoro articolo 29 è un organo europeo, istituito dalla Direttiva 95/46, che sarà sostituito dal nuovo Regolamento dal Comitato europeo per la protezione dei dati

[2] Cfr. art. 35 del Regolamento che pur non riportando una definizione formale di DPIA ne traccia il contenuto minimo e il Considerando n. 84 del Regolamento; cfr. anche Faq_Ance n. 16

Peraltro, anche laddove non si ravvisino i rischi esemplificati nelle Linee Guida quali condizioni per l'effettuazione di un DPIA, non si riduce, comunque, l'obbligo generale del titolare di ***mettere in atto tutte le misure per gestire in modo idoneo i rischi medesimi*** [3].

Si possono condurre DPIA unitarie quando diversi titolari effettuano trattamenti di dati analoghi (si pensi, ad esempio, a più aziende di un gruppo che effettuano analoghi trattamenti o agli enti bilaterali territoriali che svolgono trattamenti dati analoghi).

Ma quando il rischio si considera elevato?

A tal proposito, il WP29 elenca nelle Linee Guida alcuni ***criteri utili al fini di individuare i trattamenti dati rischiosi e suscettibili***, pertanto, di una valutazione di impatto (DPIA). A mero titolo esemplificativo, si segnalano:

- trattamenti volti a osservare, monitorare e controllare gli interessati (*si pensi agli apparecchi di videosorveglianza*);
- trattamenti di dati sensibili o di dati di natura strettamente personale (*dati trattati dai datori di lavoro e dagli enti bilaterali*);
- trattamenti di dati su larga scala (*trattamenti effettuati dagli enti bilaterali*).

Laddove il titolare, anche in presenza di uno o più dei criteri elencati nelle Linee Guida (cfr. pagg. 8/12 del documento), ritenga che comunque l'utilizzo dei dati non comporti rischi particolari, dovrà motivare e documentare la scelta della mancata conduzione di DPIA, allegando o annotando l'opinione del responsabile della protezione dati (DPO - Data Protection Officer), ove esistente.

Quando effettuare il DPIA?

Un aspetto importante che emerge dalle Linee Guida e che caratterizza la *ratio* del nuovo Regolamento è che, pur se la DPIA deve essere condotta prima che inizi il trattamento, lo svolgimento della stessa deve rappresentare anche un **processo continuativo e non un'attività una tantum del titolare,** poiché spesso i trattamenti possono evolversi e mutare in corso[4].

[3] Cfr. art. 24 del Regolamento principio dell'*Accauntabilty;* cfr anche Faq_Ance n. 14)

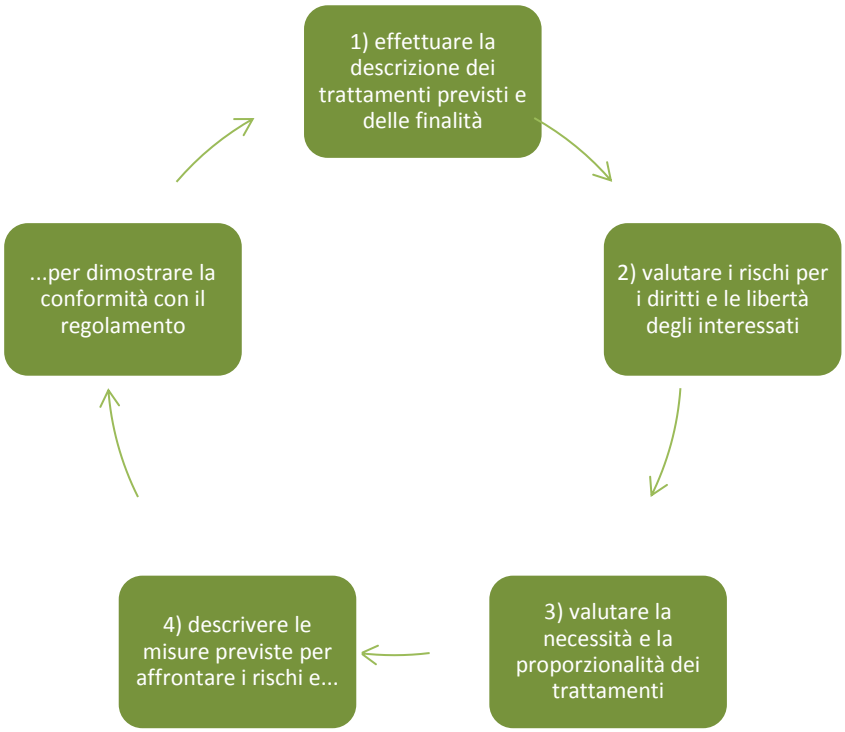
[4] Coerentemente con i principi di cui all'art. 25 del Regolamento_Data Protection by Default e by Design; cfr. anche Faq_Ance n. 15

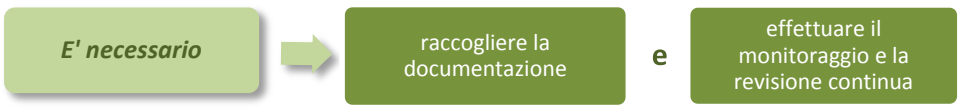
Chi effettua il DPIA?

La Valutazione di impatto deve essere effettuata dal titolare insieme al DPO e al responsabile del trattamento dei dati.

Come si effettua la DPIA?

La DPIA può essere effettuata con metodologie diverse ma secondo i seguenti medesimi criteri:





Sanzioni

La mancata effettuazione della DPIA, laddove necessaria, comporta una sanzione amministrativa fino a un massimo di 10 milioni di euro e, se si tratta di un'impresa, fino al 2% del fatturato globale annuo.

Per concludere

Dalle Linee Guida si evince la necessità di effettuare una valutazione circa l'esistenza delle condizioni richieste dal Regolamento per l'effettuazione della DPIA nel trattamento dei dati, utile al fine di dimostrare la corretta *compliance* alla normativa in tema di Tutela della Privacy.

È bene evidenziare che certamente nell'ambito di piccole imprese non sarà necessario adottare la procedura di cui sopra, pur ritenendosi prudenziale portare comunque avanti una valutazione del caso per scongiurare ogni rischio.

Diversamente nel caso delle grandi imprese, delle associazioni territoriali o degli enti bilaterali, i quali dovranno procedere, senza alcun dubbio, ad una DPIA.