

*ADAPT - Scuola di alta formazione sulle relazioni industriali e di lavoro  
Per iscriverti al Bollettino ADAPT [clicca qui](#)  
Per entrare nella **Scuola di ADAPT** e nel progetto **Fabbrica dei talenti**  
scrivi a: [selezione@adapt.it](mailto:selezione@adapt.it)*

**Uno dei principali adempimenti previsti dal nuovo Regolamento Generale sulla Protezione dei Dati personali** (di seguito GDPR) **è quello della realizzazione, in determinati casi, di una valutazione d'impatto sulla protezione dei dati** (o *Data Protection Impact Assessment*, DPIA): essa viene definita dal Gruppo di lavoro ex art. 29 come “un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali”. (Gruppo di lavoro ex art. 29 per la protezione dei dati, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento “possa presentare un rischio elevato” ai fini del regolamento (UE) 2016/679*).

**È bene sottolineare già in principio che non si tratta di una mera formalità**, ma dell'attività preliminare per giungere al pieno rispetto della normativa prevista dal Regolamento in parola. Questo istituto, infatti, mira ad imporre un'analisi ponderata delle attività svolte nei confronti dei dati personali degli interessati già dalla fase di predisposizione dei processi al fine di implementare delle misure di sicurezza idonee anche alla luce dei principi di *privacy by design* e *privacy by default*.

**La realizzazione della valutazione d'impatto, inoltre, non deve essere considerata un adempimento *una tantum*, ma deve essere parte di un processo da integrare nel complesso delle attività aziendali.** Come previsto dall'art. 35, comma 11, GDPR, infatti, “se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentate dalle attività relative al trattamento”.

Questo aspetto rende evidente come risulti fondamentale la presenza di personale qualificato in grado di riconoscere se si renda necessario un adeguamento della valutazione d'impatto ([G. Machì](#),

*L'importanza della formazione dei lavoratori per la protezione dei dati personali, Bollettino Adapt n. 21/2017*) e, al contempo, processi organizzativi che portino i diversi soggetti coinvolti nelle attività di trattamento ad interpellare tale personale laddove sia ipotizzabile l'insorgenza di variazione del rischio.

**È evidente come la nuova disciplina si basi interamente sul concetto di *accountability*** per cui la responsabilizzazione del titolare del trattamento non si sostanzia solo nel rispetto della normativa, ma anche nella sua capacità di dimostrare di averla rispettata (L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati*, Giuffrè, Milano, 2016).

**Il focus posto sulla tutela dei diritti degli interessati rende la valutazione d'impatto sulla protezione dei dati un ottimo strumento per garantire agli *stakeholder* una particolare attenzione alla protezione dei loro dati** e per ottenere, di conseguenza, vantaggi reputazionali e competitivi (*Information Commissioner's Office, Consultation: GDPR DPIA guidance*).

**I casi in cui è necessario effettuare la valutazione d'impatto sulla protezione dei dati si possono desumere dai commi 1 e 3 dell'articolo 35 del Regolamento: mentre il primo individua il criterio di ordine generale, il terzo comma fornisce un elenco non esaustivo di trattamenti che richiedono di procedere alla valutazione d'impatto.** In termini generali, la valutazione d'impatto è richiesta «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche [...]» (così l'art. 35 comma 1 del Regolamento (UE) 2016/679).

È, quindi, in ragione del rischio connesso al trattamento che occorre valutare la necessità di procedere ad una valutazione d'impatto: a questo fine riferimenti fondamentali risultano essere, per espressa previsione normativa, la natura, l'oggetto, il contesto e le finalità del trattamento.

Quanto invece ai trattamenti per cui è lo stesso art. 35 (al comma 3) a prevedere la necessità della valutazione d'impatto, si tratta dei seguenti casi:

«**Valutazione sistematica** e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo sistematicamente su dette persone fisiche» (lettera a);

**Trattamento su larga scala di dati** relativi a condanne penali e reati e su dati «che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (lettera b);

**Sorveglianza sistematica su larga scala di una zona accessibile al pubblico** (lettera c).

**Tra le attività di trattamento che possono richiedere la necessità di una valutazione d'impatto sulla protezione dei dati personali vi sono quelle relative ai dati dei lavoratori. Tale operazione può comportare diversi rischi specifici relativi allo status di lavoratore:** dalla discriminazione alla possibilità di ottenere una valutazione del proprio rendimento professionale non coerente con la realtà (considerando 75).

**L'aspetto principale che rende particolare il trattamento dei dati dei lavoratori è il contesto del trattamento:** il fatto che le informazioni dei lavoratori siano trattate, direttamente (dal *recruiting* alle gestione delle questioni fiscali) o indirettamente (attività di videosorveglianza), in funzione del rapporto di lavoro è molto rilevante dal punto di vista dell'equilibrio dei poteri tra interessato e titolare del trattamento (*Gruppo di lavoro ex art. 29 per la protezione dei dati, Opinion 2/2017 on data processing at work - wp249*).

La posizione di inferiorità dei lavoratori, talvolta definiti anche “soggetti vulnerabili” ([Gruppo di lavoro ex art. 29 per la protezione dei dati, Linee guida in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il trattamento “possa presentare un rischio elevato” ai fini del regolamento \(UE\) 2016/679](#)), nei confronti del datore di lavoro può, ad esempio, rendere più difficoltoso l’esercizio dei diritti del lavoratore-interessato regolati al capo III del Regolamento in esame.

**Vi sono molteplici casi di trattamento dei dati dei lavoratori che devono essere necessariamente soggetti a valutazione d’impatto** poiché rientrano nelle casistiche previste dall’art. 35, comma 3, GDPR sopra esposto o perché, comunque, riconducibili alla nozione espressa al comma 1. Si pensi, per esempio, a tutte le operazioni di *people analytics* ([E. Dagnino, People Analytics: lavoro e tutele al tempo del data management tramite big data, Labour Law and Issues, 2017](#)) a supporto, ad esempio, della funzione di *recruiting* che possono essere ricondotti ai casi di valutazione sistematica regolati alla lettera a); o all’utilizzo di informazioni biometriche, in particolare le impronte digitali e la scansione dell’iride, spesso utilizzati nei sistemi d’accesso a particolari luoghi di lavoro e che potrebbero rientrare nei casi previsti alla lettera b); o, ancora, alle attività di sorveglianza dei lavoratori che offrono la propria prestazione lavorativa in centri commerciali o altri luoghi aperti al pubblico, riconducibili, invece, alla lettera c). Altri esempi di trattamenti che possono richiedere la valutazione d’impatto sono offerti dalla Opinion 2/2017 e dalle linee guida in materia di valutazione d’impatto citate.

Emerge, di conseguenza, l’importanza di questo obbligo anche nel trattamento dei dati dei lavoratori, un obbligo che, insieme agli altri previsti dalla disciplina in materia di protezione dei dati personali, va ad integrare quanto previsto dalle discipline giuslavoristiche alla luce degli artt. 8 e 15 dello Statuto dei lavoratori per ciò che concerne il divieto di indagine sulle opinioni personale del lavoratore e il divieto di discriminazione ed all’art. 4 della medesima legge per ciò che concerne l’attività di controllo a distanza ([E. Dagnino, Tecnologie e controlli a distanza, DRI, 4/2015](#)).

**Infine, dalla lettura del comma 9 dell’articolo 35, si potrebbe ipotizzare un possibile spazio di intervento anche per le rappresentanze dei lavoratori.** Si prevede infatti, che i rappresentanti degli interessati dovranno essere consultati dal titolare salvo che ciò sia impossibile o vada a detrimento degli stessi diritti che si vogliono tutelare. In questi casi, tuttavia, è opportuno che la scelta di non effettuare tali consultazioni sia giustificata e documentata in ossequio al principio di *accountability* ([Gruppo di lavoro ex art.29 per la protezione dei dati, Linee guida in](#)

*materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679).*

Un intervento del sindacato può servire ad attenuare lo squilibrio tra titolare-datore di lavoro e interessato-lavoratore e, nel caso specifico della valutazione d'impatto, può essere utile sia a dar voce alle istanze dei lavoratori che ad aumentare l'accettabilità delle pratiche utilizzate dai datori per il trattamento dei loro dati. Rimane fermo anche l'interesse di questi ultimi al mantenimento di una sorta di *accountability* interna allo scopo di ottenere una maggiore attrattività nei confronti delle migliori risorse presenti nel mercato del lavoro che, col passare del tempo, acquisiscono una sempre maggiore consapevolezza delle operazioni che vengono effettuate sui loro dati.

**Gaetano Machì**

ADAPT Junior Fellow

 @Gae95

Scarica il **PDF** 