DECRETO TRASPARENZA: QUALE RICADUTA SU ADEMPIMENTI GDPR
D.Lgs 27 giugno 2022 n. 104

Entra in vigore il decreto che disciplina il diritto all'informazione sugli elementi essenziali del rapporto di lavoro, sulle condizioni di lavoro e la relativa tutela.
Pesante, la ricaduta sugli adempimenti aziendali, in particolare sull'attività di revisione dei contratti e sulla documentazione informativa verso dipendenti e collaboratori.

Dal 1 agosto, il cosiddetto Decreto trasparenza, sarà applicato a chi ha già un contratto in corso e dal 13 agosto ai nuovi assunti. La legge, recepisce la Direttiva UE 2019/1153 relativa a condizioni di lavoro trasparenti e prevedibili.

L'obbligo di fornire informazioni, su richiesta del lavoratore, non è una novità per la materia giurislavoristica né per la normativa sulla protezione dei dati personali. Tuttavia, ai fini del GDPR, risulta particolarmente interessante l'art. 1 bis - Ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati dove si recita che *il datore di lavoro o il committente pubblico o privato è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonchè indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.*

Il testo, fa chiaramente riferimento a strumenti informatici e sistemi decisionali o di monitoraggio automatizzati utilizzati dal datore di lavoro prima dell'assunzione e durante lo svolgimento dell'attività lavorativa. Aspetto questo, già richiamato dai Considerando 71 e 72 collegati all'art. 22 del GDPR che fa riferimento ai diritti dell'interessato a *non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*.

Per quanto sopra, il datore di lavoro o il committente è tenuto a fornire al lavoratore, unitamente alle informazioni tipiche del rapporto di lavoro elencate nel documento di legge, prima dell'inizio dell'attività lavorativa, anche le seguenti informazioni:
a) gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi (organizzativi ed informatici);
b) gli scopi e le finalità dei sistemi;
c) la logica ed il funzionamento dei sistemi;
d) le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi inclusi i meccanismi di valutazione delle prestazioni;
e) le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità;
f) il livello di accuratezza, robustezza e cybersicurezza dei sistemi (informatici ed organizzativi) e le metriche utilizzate per misurare tali parametri, nonchè gli impatti potenzialmente discriminatori delle metriche stesse.

Interessante, il riferimento alle *metriche utilizzate* per evitare discriminazioni ovvero alla presenza di quegli algoritmi presenti, principalmente nei software di selezione e gestione delle risorse umane, noti come HR Application ed amministrazione del personale (es. paghe e contributi) ma anche negli strumenti di Business Intelligence utilizzati per estrapolare informazioni dai dbase aziendali compreso l'arcinoto Excel al fine di profilare un potenziale candidato o un dipendente per misurare le sue prestazioni. Chiaro il riferimento al principio *privacy by design* che prevede la necessità di tutelare i dati, in questo caso dei lavoratori, fin dalla fase di progettazione dei sistemi che ne prevedono la raccolta e l'utilizzo.

A tal proposito, si ricorda che il ricorso all'istituto del consenso privacy per semplificare l'accettazione delle *metriche* non potrà mai essere valido se non è possibile comprendere le modalità di trattamento tramite algoritmo (Cassazione sentenza n. 14381/2021).

Altro aspetto interessante è laddove si legge: *Il datore di lavoro o il committente sono tenuti a integrare l'informativa con le istruzioni per il lavoratore in merito alla sicurezza dei dati e l'aggiornamento del registro dei trattamenti riguardanti le attività di cui al comma 1, incluse le attività di sorveglianza e monitoraggio. Al fine di verificare che gli strumenti utilizzati per lo svolgimento della prestazione lavorativa siano conformi alle disposizioni previste dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, il datore di lavoro o il committente effettuano un'analisi dei rischi e una valutazione d'impatto degli stessi trattamenti, procedendo a consultazione preventiva del Garante per la protezione dei dati personali ove sussistano i presupposti di cui all'articolo 36 del Regolamento medesimo.*

Pertanto, andranno aggiornati ed in mancanza, prodotti:

1. L'informativa, come da art.13 del GDPR nei confronti di dipendenti e collaboratori;
2. La lettera di incarico come da Considerando 81 ed art. 29 del GDPR con indicazioni relative alla sicurezza;
3. Il Registro delle attività di trattamento del titolare (art. 30) e la parte relativa all'analisi dei rischi di trattamento;
4. La valutazione d'impatto sulla protezione dei dati personali (art. 35) relativa ai trattamenti con strumenti informatici e sistemi decisionali o di monitoraggio automatizzati.

Quindi, la norma evidenza la sua dinamicità quando prescrive che in costanza di rapporto con l'azienda, se vi fossero aggiornamenti per elementi non noti quali leggi e contratti collettivi (si pensi ad esempio a nuovi orari interni o sviluppo di nuovi software di monitoraggio rete) questi andranno comunicati ai lavoratori entro il primo giorno dal loro effetto.

Il diritto di accesso ai dati, sancito dall'art. 15 del GDPR, è sempre esercitabile dal lavoratore, *direttamente o per il tramite delle rappresentanze sindacali aziendali o territoriali anche al fine di richiedere ulteriori informazioni relative ai nuovi obblighi*. Tanto che il datore di lavoro o il committente sono tenuti a trasmettere i dati richiesti ed a rispondere per iscritto entro trenta giorni.

Inoltre, non è da trascurare, nell'elenco degli elementi essenziali del rapporto di lavoro, il richiamo al diritto del lavoratore a ricevere la *formazione erogata dal datore di lavoro, se prevista*. Questa indicazione emerge tra le righe dell'art. 29 del GDPR (*chiunque abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso)* e nell'art. 39 (compiti del Responsabile della protezione dei dati personali, anche noto come DPO) e va interpretata come una ulteriore misura che contribuisce a quella *robustezza e cybersicurezza dei sistemi* richiamata alla lettera f) dell'art. 1 bis di questo decreto.

Le aziende e gli studi professionali che hanno adottato delle policy interne per rispettare il noto principio dell'*accountability* nonché quello della *trasparenza* non dovrebbero avere ricadute significative. Tuttavia, chi ha prodotto documenti generici ovvero privi di indicazioni puntuali verso i lavoratori non tenendo conto, per esempio, della mansione (es. lettere di incarico autorizzato al trattamento) o adottando informative ex art. 13 generiche, dovrà fare una significativa attività di revisione documentale per non incorrere nelle pesanti sanzioni previste per le inadempienze.

Le violazioni, accertate dagli Uffici competenti, anche su denuncia del lavoratore, sono punite con una rafforzata sanzione amministrativa da 250 a 1.500 euro per ciascun lavoratore, a cui si aggiunge un'ulteriore sanzione qualora non siano rispettati gli ulteriori specifici obblighi informativi riservati ai contratti basati sull'utilizzo di sistemi decisionali o di monitoraggio automatizzati (da 100 a 750 euro per ciascun mese, elevata fino a 1.000-5.000 euro se la violazione si riferisce a più di 10 lavoratori).

Luigi Rendina
DPO e Consulente privacy
Linkedin