

Newsalert

Data Protection and Privacy, Labour and Executive Compensation

Decreto Trasparenza: chiarimenti interpretativi del Garante in merito agli obblighi *data protection*

Introduzione

L'Autorità Garante per la protezione dei dati personali ("Garante") ha recentemente pubblicato sul proprio sito internet un documento volto a fare luce su taluni questioni interpretative e applicative in materia di protezione dei dati connesse all'entrata in vigore del d. lgs. 27 giugno 2022, n. 104 (c.d. "Decreto Trasparenza").

Come noto, tale intervento legislativo ha introdotto nel nostro ordinamento una serie di obblighi in capo ai datori di lavoro che utilizzino sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni (i) 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, e che, dunque, siano finalizzati a realizzare un procedimento decisionale in grado di incidere sul rapporto di lavoro, ovvero (ii) incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori.

Le indicazioni del Garante fanno seguito ai chiarimenti forniti in precedenza, per i profili di loro competenza, dal Ministero del Lavoro e delle Politiche Sociali (con circolare n. 19 del 20/9/2022) e dall'Ispettorato Nazionale del Lavoro (con circolare n. 4 del 10/8/2022), al fine di coordinare le reciproche posizioni e le linee interpretative in merito all'applicazione del Decreto Trasparenza nel suo rapporto con gli obblighi previsti dal Regolamento (UE) 679/2016 ("GDPR") e dal D.lgs. n. 196/2003 ("Codice Privacy").

A tali fini, il Garante individua tra gli obblighi informativi contenuti nel Decreto Trasparenza: **(a)** taluni elementi informativi **ulteriori** e **integrativi** rispetto a quelli previsti dagli artt. 13 e 14 del GDPR¹, nonché **(b)** taluni elementi informativi che **specificano** la portata di quanto già previsto dagli artt. 13 e 14 del GDPR².

¹ È questo il caso delle informazioni circa gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi decisionali o di monitoraggio automatizzati, il funzionamento dei sistemi e i parametri principali utilizzati per programmarli o addestrarli, le misure di controllo adottate per le decisioni, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità, il livello di accuratezza, robustezza e cybersicurezza dei sistemi e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.

² È questo il caso delle informazioni circa la logica dei sistemi decisionali o di monitoraggio automatizzati (espressamente previste dal GDPR in caso di ricorso a processi decisionali automatizzati, compresa la profilazione), nonché l'indicazione delle categorie di dati trattati (prevista nel GDPR solo ove i dati oggetto di trattamento non siano ottenuti presso l'interessato).

Le indicazioni del Garante e gli obblighi in capo ai datori di lavoro

Di seguito sono riportati i principali punti di attenzione che emergono dai chiarimenti del Garante in relazione agli obblighi *data protection* posti in capo ai datori di lavoro-titolari del trattamento:

- **Ambito di applicazione soggettiva.** In primo luogo, sebbene le disposizioni del Decreto Trasparenza si applichino esclusivamente alle tipologie di rapporti di lavoro che lo stesso individua al proprio art. 1, i datori di lavoro sono comunque tenuti al rispetto della disciplina generale in materia di protezione dei dati personali anche in relazione ai rapporti di lavoro esclusi dall'applicazione del Decreto.
- **Assolvimento degli obblighi informativi per i rapporti di lavoro instaurati successivamente al 1° agosto 2022.** Il Garante ritiene auspicabile che, nel medesimo termine previsto dal Decreto Trasparenza (i.e., prima dell'inizio dell'attività lavorativa), siano fornite al dipendente anche le informazioni di cui agli artt. 13 e 14 del GDPR. In ottica di semplificazione degli adempimenti e per evitare la frammentazione informativa, tali informazioni andranno rese, congiuntamente, nell'ambito dello stesso documento.
- **Assolvimento degli obblighi informativi per i rapporti di lavoro già instaurati al 1° agosto 2022.** In merito a tali rapporti, il Decreto Trasparenza prevede che i dipendenti possano ottenere le informazioni a seguito di specifica richiesta scritta al datore di lavoro, che dovrà riscontrare la stessa entro 60 giorni. Sul punto, il Garante sembra suggerire che il dipendente possa comunque, nell'esercizio del diritto di accesso ai propri dati personali di cui al GDPR, ottenere le ulteriori informazioni di cui al Decreto Trasparenza anche con le modalità e nella tempistica più breve previsti al riguardo dal GDPR stesso (cfr., in particolare, il termine massimo di 30 giorni di cui all'art. 12 GDPR).
- **Presupposti di liceità del trattamento.** Il datore di lavoro, nella sua veste di titolare del trattamento, dovrà verificare la sussistenza di un presupposto di liceità di cui all'art. 6 del GDPR prima di poter fare ricorso ai sistemi di cui al Decreto Trasparenza. In forza dei richiami negli artt. 113-114 del Codice Privacy, il datore dovrà inoltre: (i) assicurarsi il ricorrere dei presupposti di liceità di cui all'art. 4 dello Statuto dei Lavoratori, e (ii) rispettare il divieto di acquisire e trattare informazioni e fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore o afferenti alla sua sfera privata di cui all'art. 8 dello Statuto.
- **Rispetto dei principi del trattamento.** Il datore di lavoro dovrà rispettare i principi generali del trattamento di cui all'art 5 GDPR (ivi inclusi quelli di liceità, correttezza e trasparenza del trattamento; di limitazione delle finalità; di minimizzazione, esattezza e aggiornamento dei dati; di limitazione della conservazione e di integrità e riservatezza).
- **Accountability e DPIA.** In ossequio al principio di *accountability*, il datore di lavoro dovrà valutare la necessità di effettuare una *Data Protection Impact Assessment* (DPIA) ai sensi dell'art. 35 GDPR nel caso in cui i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenendo conto delle indicazioni fornite dallo *European Data Protection Board*.
- **Data Protection by design e by default.** Ai sensi dell'art. 25 GDPR, il datore di lavoro dovrà inoltre adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (*data protection by design*), nonché garantire che, per impostazione predefinita, vengano eseguiti i soli trattamenti di dati strettamente necessari per la specifica finalità perseguita (*data protection by default*).
- **Registro dei trattamenti e Informativa.** Il datore di lavoro dovrà altresì aggiornare il proprio registro dei trattamenti ai sensi dell'art. 30 GDPR, nonché integrare l'informativa con le istruzioni per il lavoratore in merito alla sicurezza dei dati.
- **Processi decisionali unicamente automatizzati.** Ove i sistemi diano luogo ad un processo decisionale unicamente automatizzato (compresa la profilazione) che produca effetti giuridici o che incida significativamente sull'interessato, il datore di lavoro dovrà assicurare il rispetto dell'art. 22 del GDPR, valutando e strutturando processi alternativi che consentano il diritto di ottenere l'intervento umano e di contestare la decisione.

II Sintesi delle attività da svolgere da parte dei datori di lavoro

Per pronto riferimento, di seguito sono sintetizzate le attività richieste al datore di lavoro per conformarsi alla disciplina in materia di protezione dei dati personali in relazione al Decreto Trasparenza:

- analizzare i propri processi interni al fine di individuare possibili processi decisionali automatizzati. Questi, infatti, possono essere presenti in numerosi processi aziendali, come, ad esempio, l'assegnazione o la revoca automatizzata di compiti, mansioni o turni, o la definizione dell'orario di lavoro;
- accertarsi che i processi decisionali automatizzati rispecchino i principi applicabili al trattamento, tra cui quelli di *privacy by design* e *privacy by default*;
- valutare la necessità di effettuare una *Data Protection Impact Assessment* (DPIA) ai sensi dell'articolo 35 del GDPR. Tale attività è necessaria al fine di analizzare e, di conseguenza gestire, possibili rischi per i diritti e le libertà delle persone fisiche;
- nel caso in cui ne ricorrano i presupposti, procedere con una consultazione preventiva di cui all'articolo 36 del GDPR;
- modificare le informative privacy al fine di fornire, in maniera chiara e trasparente, le informazioni indicate dalla normativa;
- aggiornare le designazioni ai sensi dell'articolo 29 del GDPR affinché queste riflettano eventuali nuovi obblighi in materia di sicurezza;
- aggiornare il registro delle attività di trattamento;
- verificare e, se del caso, aggiornare i contratti con i fornitori dei suddetti Processi Decisionali Automatizzati, nominandoli responsabili del trattamento ex articolo 28 del GDPR;
- In caso i fornitori si trovassero al di fuori dell'EEA, valutare la necessità di effettuare un *Data Transfer Assessment* per garantire la corretta esportazione extra-UE dei dati personali;
- valutare e strutturare processi alternativi che consentano il diritto di ottenere l'intervento umano e di contestare la decisione, come richiesto dalla normativa applicabile.

Contatti

Data Protection & Privacy
newsletter.dataprotection@chiomenti.net

Labour and Executive Compensation
newsletter.lavoro@chiomenti.net
