Garante privacy: protezione dei dati personali e decreto Trasparenza – Nota di approfondimento

Si informa che il Garante per la protezione dei dati personali ha fornito, sul proprio portale, le prime indicazioni in materia di protezione dei dati connesse all'entrata in vigore del d.lgs. n. 104/2022 (c.d. decreto Trasparenza), che si riportano di seguito.

Interazione del nuovo quadro regolatorio con la disciplina di protezione dei dati personali

In via preliminare, il Garante della privacy ha ricordato che il decreto Trasparenza ha introdotto ulteriori obblighi informativi qualora il datore di lavoro utilizzi *"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 nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori"* (cfr. comunicazione Ance del 2 agosto 2022).

L'Autorità ha precisato che la disciplina del citato decreto deve essere necessariamente coordinata, in sede applicativa, con la normativa in materia di protezione dei dati personali[1].

Tale esigenza si evince altresì da quanto indicato nello stesso Decreto laddove specifica che resta salva "*la configurabilità di eventuali violazioni in materia di protezione dei dati personali ove sussistano i presupposti di cui agli articoli 83 del Regolamento UE 2016/679 e 166 del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni*".

Nuovi obblighi informativi

Il nuovo art. 1-bis, introdotto dal decreto Trasparenza, indica le ulteriori informazioni – in aggiunta a quanto previsto dagli artt. 13 e 14 del Regolamento (UE) 2016/679 – che il datore di lavoro ha l'obbligo di fornire al lavoratore, qualora tratti dati personali attraverso i predetti sistemi decisionali o di monitoraggio automatizzati.

Tra le informazioni ulteriori che il datore di lavoro, in qualità di titolare del trattamento, deve fornire all'interessato rientrano: gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi decisionali o di monitoraggio automatizzati; il funzionamento dei sistemi; i parametri principali utilizzati per programmare o addestrare i sistemi decisionali o di monitoraggio automatizzati, inclusi i meccanismi di valutazione delle prestazioni; le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della

[1] Regolamento (UE) 2016/679; d. lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

qualità; il livello di accuratezza, robustezza e cybersicurezza dei sistemi decisionali o di monitoraggio automatizzati e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.

Tra gli elementi che, invece, specificano quanto già compreso negli artt. 13 e 14 del Regolamento, rientrano: la logica dei sistemi decisionali o di monitoraggio automatizzati; l'indicazione delle categorie di dati trattati.

Il momento entro il quale devono essere assolti gli obblighi informativi

Il Garante della privacy ha ricordato che le disposizioni del Decreto si applicano a tutti i rapporti di lavoro, anche a quelli già instaurati alla data del 1° agosto 2022.

Con riguardo ai rapporti di lavoro instaurati anteriormente a tale data, è previsto che i dipendenti possano ottenere i predetti elementi informativi a seguito di specifica richiesta scritta rivolta al datore di lavoro.

Con riferimento ai rapporti di lavoro instaurati successivamente a tale data, gli obblighi informativi aggiuntivi devono essere adempiuti prima dell'inizio dell'attività lavorativa.

In applicazione del principio di liceità, correttezza e trasparenza[2], il Garante della privacy ha ritenuto auspicabile che tutte le informazioni vengano fornite complessivamente al lavoratore prima dell'inizio del trattamento, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro[3], nonché in formato strutturato, di uso comune e leggibile da dispositivo automatico[4].

Inoltre, il Garante della privacy ha consigliato di fornire le specifiche informazioni sui sistemi decisionali o di monitoraggio automatizzati congiuntamente (ossia nello stesso documento) alle informazioni di cui agli artt. 13 e 14 del citato Regolamento UE.

Sistemi decisionali o di monitoraggio automatizzati

Considerato che l'impiego di sistemi decisionali o di monitoraggio automatizzati può comportare il trattamento d'informazioni associate in via diretta o indiretta ai dipendenti, il Garante della privacy ha chiarito che occorre, in ogni caso, che il titolare del trattamento verifichi la sussistenza di un idoneo presupposto di liceità[5].

[2] Art. 5, par. 1, lett. a), Regolamento (UE) 2016/679.
[3] Art. 12, Regolamento (UE) 2016/679.
[4] Art. 1-bis, d.lgs. n. 152/1997.
[5] Artt. 5, par. 1, lett. a) e 6 del Regolamento (UE) 2016/679.

Il datore di lavoro, titolare del trattamento, deve pertanto rispettare le condizioni per il lecito impiego di strumenti tecnologici nel contesto lavorativo[6].

Nel dettaglio, dovrà essere sempre verificata la sussistenza dei presupposti di liceità stabiliti dall'art. 4 della l. 20 maggio 1970, n. 300, cui fa rinvio l'art. 114 del Codice in materia di protezione dei dati personali, nonché il rispetto delle diposizioni che vietano al datore di lavoro di acquisire e trattare informazioni e fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore o afferenti alla sua sfera privata.

Il Garante della Privacy ha, inoltre, chiarito che gli artt. 113 e 114 del predetto Codice sono considerati disposizioni più specifiche e di maggiore garanzia rispetto all'art. 88 del Regolamento UE, la cui osservanza costituisce una condizione di liceità del trattamento e la cui violazione determina l'applicazione di sanzioni amministrative pecuniarie ai sensi dell'art. 83, par. 5, lett. d) del Regolamento.

Il Garante della privacy ha precisato che il titolare del trattamento è tenuto a rispettare i principi generali del trattamento[7] e a porre in essere tutti gli adempimenti previsti dalle disposizioni normative in materia di protezione dei dati personali.

Inoltre, in attuazione del principio di responsabilizzazione[8], spetta al titolare valutare se i trattamenti che si intende realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali[9].

Al fine di verificare la sussistenza dell'obbligo di procedere ad una valutazione di impatto, il titolare deve tenere conto delle indicazioni fornite anche a livello europeo, come:

- la particolare "vulnerabilità" degli interessati nel contesto lavorativo[10];
- l'impiego di sistemi che comportano il "monitoraggio sistematico" (inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti")[11].

Il Garante della privacy ha, inoltre, chiarito che possono venire in rilievo anche altri criteri individuati dal Comitato europeo per la protezione dei dati ai fini della valutazione. Ad esempio: valutazione o assegnazione di un punteggio; processo decisionale automatizzato che ha effetto giuridico o incide

[6] Art. 88, par. 2, del Regolamento (UE) 2016/679.
[7] Art. 5, Regolamento (UE) 2016/679.
[8] Artt. 5, par. 3, 24 e 25, Regolamento (UE) 2016/679.
[9] Art. 35, Regolamento (UE) 2016/679.
[10] Art. 88, Regolamento (UE) 2016/679; "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679", WP 248 del 4 aprile 2017, che, tra le categorie di interessati vulnerabili, menziona espressamente "i dipendenti";
[11] Artt. 35 e 88, par. 2, Regolamento (UE) 2016/679.

in modo analogo significativamente; trattamento di dati su larga scala; creazione di corrispondenze o combinazione di insiemi di dati; uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Sul punto, il Garante della privacy ha ricordato che, nella maggior parte dei casi, un trattamento che soddisfa almeno due criteri deve essere oggetto della valutazione d'impatto sulla protezione dei dati e che maggiore è il numero di criteri soddisfatti dal trattamento e più è probabile che si configuri un rischio elevato per i diritti e le libertà degli interessati.

Fermo restando quanto sopra, la redazione della valutazione d'impatto è sempre obbligatoria qualora si faccia ricorso a "*una 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 significativamente su dette persone fisiche*"[12].

Il Garante della privacy ha evidenziato che, in tale quadro, dovrà essere rispettato altresì il principio della "*protezione dei dati fin dalla progettazione*"[13] mediante l'adozione di misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati[14] e integrando nel trattamento le necessarie garanzie per tutelare i diritti e le libertà degli interessati.

Il trattamento dovrà essere, inoltre, conforme al principio della "*protezione dei dati per impostazione predefinita*"[15], ponendo in essere scelte tali da garantire che venga effettuato, per impostazione predefinita, solo il trattamento strettamente necessario per conseguire una specifica e lecita finalità.

Dunque, il titolare del trattamento non deve raccogliere dati personali che non siano necessari per la specifica finalità del trattamento[16].

In attuazione dei suddetti principi, il titolare del trattamento, anche quando utilizza sistemi tecnologici realizzati da terzi, dovrà eseguire, avvalendosi del supporto del responsabile della protezione dei dati, ove nominato, un'analisi dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica, non sono compatibili con le finalità del trattamento, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento.

Successivamente, il Garante della privacy ha ricordato che il Regolamento europeo prevede l'obbligo in capo al titolare del trattamento di redigere il registro delle attività di trattamento al

[12] Art. 35, par. 3, lett. a), Regolamento (UE) 2016/679.
[13] Art. 25, par. 1, Regolamento (UE) 2016/679.
[14] Art. 5, Regolamento (UE) 2016/679.
[15] Art. 25, par. 2, del Regolamento (UE) 2016/679.
[16] "Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 42, 44 e 49.

ricorrere dei relativi presupposti[17]. Tale registro è indispensabile per consentire al titolare di censire i trattamenti effettuati e documentarne la conformità alla disciplina in materia di protezione dei dati personali.

Considerata la funzione del registro, visto l'art. 1-bis, comma 4, del d.lgs. n. 152/1997[18], il Garante della privacy ha chiarito che il titolare del trattamento non è tenuto a informare gli interessati della predisposizione del registro e di ogni aggiornamento dello stesso.

Infine, il Garante della privacy ha precisato che occorre valutare se i sistemi impiegati diano luogo a un processo decisionale unicamente automatizzato, compresa la profilazione, che produca effetti giuridici o che incida significativamente sull'interessato.

In questi casi trova applicazione l'art. 22 del Regolamento europeo che disciplina:

- le ipotesi in cui il diritto di non essere sottoposto a tali trattamenti può essere derogato;
- le garanzie per l'interessato (il diritto di ottenere l'intervento umano da parte del titolare del trattamento, il diritto di esprimere la propria opinione e il diritto di contestare la decisione).

Per quanto non riportato, si rimanda alla Nota allegata.

[17] Art. 30, Regolamento (UE) 2016/679.

[18] "*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*".