Newsletter FEBBRAIO 2018

PRECEDENTI NAZIONALI IN TEMA DI *PRIVACY:*
Conformarsi alla normativa sulla *privacy* non è una mera formalità, ma richiede l'adozione di adeguati meccanismi di *governance*

Di recente, il Garante per la protezione dei dati personali ("**Garante**") e la Corte di Cassazione hanno adottato una serie di interessanti decisioni, che chiariscono l'approccio da seguire in merito ad alcune tematiche, anche in vista dell'entrata in vigore del *General Data Privacy Regulation*[1] ("**GDPR**"). In sintesi, e in via di anticipazione su quanto sarà esposto qui di seguito in maggior dettaglio, le imprese sono chiamate a un esercizio di ridefinizione della propria organizzazione interna, per valutare, tra l'altro, se e come (i) istituire nuove funzioni societarie (come il DPO), (ii) rivedere le relazioni con i dipendenti ai sensi di nuove *privacy policy* e (iii) mettere in atto specifiche protezioni nei rapporti con i fornitori esterni.

1. Un nuovo organismo di controllo: il *Data Protection Officer*

Il 15 dicembre 2017 il Garante, al fine di accompagnare gli enti pubblici nel complesso percorso di adeguamento ai nuovi istituti previsti dal GDPR, ha pubblicato alcune FAQ sulla funzione del Responsabile della Protezione dei Dati (*Data Protection Officer*, "**DPO**") nel settore pubblico.

Anche se si focalizzano sul settore della pubblica amministrazione, le FAQ contengono una serie di principi e indicazioni generali che possono, però, essere utili per tutte le imprese che dovranno nominare un DPO.

Più nel dettaglio, le FAQ forniscono i seguenti chiarimenti.

- L'art. 37 del GDPR prevede che i titolari e i responsabili del trattamento designino un DPO "*quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico*", senza, tuttavia, fornire una definizione di autorità o organismo pubblico. Le FAQ chiariscono che al di là di tutti gli enti pubblici nazionali, è fortemente raccomandato che anche soggetti privati che esercitano funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), procedano alla designazione di un DPO.
- Nel caso in cui il DPO sia un dipendente, secondo le FAQ, è preferibile che la designazione sia conferita a un dirigente, ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza. Inoltre, le FAQ specificano che non sono necessarie particolari certificazioni per essere nominati quali DPO.
- Il DPO deve essere nominato con un atto di designazione formale che ne indichi le generalità, i compiti e le funzioni, e che contenga un breve riassunto delle motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio DPO.
- Il DPO dovrà essere dotato delle risorse necessarie per svolgere la sua funzione. In proposito, le FAQ precisano che ciascun ente pubblico dovrà valutare l'opportunità d'istituire un apposito ufficio, o assumere nuove risorse per assistere il DPO

1 Regolamento (EU) 2016/679 del Parlamento Europeo e del Consiglio.

nell'assolvimento dei suoi compiti. Tuttavia, le FAQ chiariscono che non è possibile nominare più di un DPO per ciascun ente pubblico.

- Le FAQ prevedono che sia possibile assegnare al DPO ulteriori compiti e funzioni, a condizione che non diano adito a un conflitto di interessi e che consentano al DPO di avere a disposizione il tempo sufficiente per l'espletamento dei compiti previsti dal GDPR. Di conseguenza, è ragionevole che negli enti di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al DPO ulteriori responsabilità. Inoltre, secondo le FAQ, il DPO non dovrà svolgere ulteriori compiti che richiedano capacità decisionali, in ordine alle finalità e ai mezzi del trattamento di dati personali, e che possano creare situazioni di conflitto di interessi.

Come anticipato, le FAQ paiono indicare principi d'ordine generale, valevoli non solo per il settore pubblico, ma anche per quello privato. In entrambi gli ambiti, la nomina del DPO è incoraggiata dal Garante, anche in situazioni in cui non sarebbe strettamente necessaria sulla base di quanto previsto dal GDPR. È verosimile ritenere che, in caso di contenzioso, la mancata nomina di un DPO possa essere sfavorevolmente valutata dall'organo giudicante, come carenza nel rispetto degli obblighi di diligenza da parte degli amministratori della persona giuridica (come del resto è già avvenuto per la mancata nomina degli Organismi di Vigilanza previsti dal D.Lgs. 231/2001).

Le FAQ sembrano chiaramente indicare che il DPO dovrà avere l'esperienza, le capacità, le risorse e la posizione che gli consentano di svolgere le sue mansioni in modo efficiente. Questo comporterà che i Consigli di Amministrazione delle persone giuridiche dovranno procedere alle nomine sulla base di decisioni adeguatamente motivate e prevedere che i DPO siano dotati di poteri e risorse adeguati. Inoltre, tali decisioni dovranno valutare con attenzione il nuovo assetto organizzativo, per evitare rischi di sovrapposizione tra le funzioni del DPO e quelle degli altri organismi di vigilanza e controllo (basti pensare alle funzioni dell'Organismo di Vigilanza 231 nella confinante materia dei reati informatici).

2. Dipendenti

Con la sentenza n. 25147, datata 24 ottobre 2017, la Corte di Cassazione ha recentemente dichiarato legittimo il licenziamento di un dipendente per aver copiato su una *pen drive* alcuni dati di proprietà del datore di lavoro e - in tale contesto - ha colto l'occasione per ribadire i seguenti principi:

a) un dipendente può essere legittimamente licenziato dal datore di lavoro qualora violi l'obbligo di fedeltà[2]; e

b) la violazione dell'obbligo di fedeltà si verifica, *inter alia*, quando un dipendente sottrae dati aziendali dal controllo e dalla supervisione del proprio datore di lavoro.

La Corte di Cassazione afferma, peraltro, che tale condotta infedele del dipendente giustifica il licenziamento per giusta causa indipendentemente da (i) le finalità ultime perseguite dal

2 L'obbligo di fedeltà è espressamente previsto ai sensi dell'articolo 2105 cod.civ. che, tuttavia, non specifica nel dettaglio quali comportamenti siano idonei a violare tale obbligo, ragione per cui tali comportamenti sono frutto di un'elaborazione giurisprudenziale.

dipendente; (ii) l'esistenza di una perdita effettiva subita dal datore di lavoro[3]; e (iii) la circostanza che il dipendente avesse avuto libero accesso ai dati aziendali, che non erano stati dichiarati "riservati" dal datore di lavoro, direttamente o indirettamente, attraverso l'uso di *password* o di altre forme di protezione[4].

A tale riguardo, sarà comunque sempre consigliabile al datore di lavoro predisporre delle misure di sicurezza per tutelare la riservatezza dei propri dati d'impresa e, in effetti, da un punto di vista normativo, il datore di lavoro è autorizzato ad attuare alcuni rimedi volti a proteggere le informazioni aziendali dai comportamenti infedeli dei propri dipendenti. La questione è stata anche recentemente affrontata dal legislatore italiano attraverso l'approvazione del cosiddetto *Jobs Act*[5] che, *inter alia*, ammette l'uso dei cc.dd. controlli difensivi. Nella maggior parte dei casi i controlli del datore di lavoro implicano l'uso di mezzi elettronici (quali strumenti audiovisivi)[6], che non costituiscono, tuttavia, un problema nella misura in cui i datori di lavoro abbiano adottato, nella propria organizzazione d'impresa, *privacy policy* specifiche e trasparenti per i dipendenti[7], volte a regolamentare, tra gli altri:

a) modalità e limiti che caratterizzano l'uso "consentito" degli strumenti elettronici aziendali affidati al personale (inclusi i *personal computer*, gli *smartphone*, la posta elettronica, internet, ecc.);

b) l'uso delle informazioni riservate del datore di lavoro; e

c) il diritto del datore di lavoro di trattare i dati personali dei dipendenti (ad esempio accedendo ai loro *account* aziendali di posta elettronica), al fine di garantire il rispetto dell'obbligo di fedeltà e - in caso di comportamenti infedeli - di applicare le relative sanzioni (compreso il licenziamento per giusta causa).

La normativa *privacy* interagisce profondamente con il diritto del lavoro.

Le aziende dovrebbero assicurarsi di aver implementato tutti gli strumenti e le *policy* necessarie al fine di rispettare le restrizioni sulla protezione dei dati, ma anche al fine di avere la possibilità di effettuare indagini, e utilizzare l'esito dei propri *audit*, come prova nei procedimenti in materia giuslavoristica[8]. A tal scopo è essenziale l'adozione di *privacy policy* interne adeguate e, laddove necessario, di accordi con i sindacati.

3 A tal riguardo, la Corte di Cassazione ha confermato che la potenziale idoneità di un comportamento di un dipendente a violare gli interessi economici del datore di lavoro è, di per sé, sufficiente a determinare una violazione dell'obbligo di fedeltà.

4 Sarebbe irragionevole imporre al datore di lavoro il dovere di impedire ai propri dipendenti l'accesso a dati e/o informazioni aziendali che, nella maggior parte dei casi, sono necessari per lo svolgimento quotidiano dell'attività lavorativa.

5 Si fa riferimento all'articolo 4 dello Statuto dei Lavoratori (vale a dire la legge n. 300 del 20 maggio 1970).

6 Questi mezzi devono essere preventivamente autorizzati dai sindacati locali solo se, e nella misura in cui, tali mezzi consentano al datore di lavoro di eseguire un controllo a distanza sull'attività lavorativa dei dipendenti. Al contrario, in assenza di qualsiasi forma di controllo da remoto, e in base all'assunzione che i suddetti mezzi elettronici sono esclusivamente finalizzati a proteggere l'attività o le attività del datore di lavoro, non è necessario ottenere un'autorizzazione preventiva.

7 Si fa riferimento alle linee guida emesse dal Garante con la decisione n. 13 del 1° marzo 2007 sull'uso di internet e della posta elettronica.

8 Tale principio è stato, peraltro, confermato dalla Corte Europea dei Diritti Umani con la decisione del 12 gennaio 2016, emanata a seguito del ricorso no. 61496/08, che venne presentato da un cittadino rumeno contro la Romania. In particolare, la Romania venne accusata di non aver condannato un datore di lavoro che effettuò un accesso non autorizzato alle comunicazioni personali del proprio dipendente, violandone, così, il diritto alla riservatezza dei dati personali. Tale accesso venne effettuato in assenza di un'adeguata informativa preventiva concernente: (i) la sussistenza, in valore assoluto, di un diritto di accesso e di controllo da parte del datore di lavoro, rispetto alle strumentazioni aziendali messe a disposizione dei dipendenti e (ii) l'utilizzo che ciascun dipendente avrebbe potuto fare della strumentazione aziendale (ivi compreso l'eventuale divieto di uso promiscuo). In tale contesto, la Corte colse l'occasione per reiterare il seguente principio: "*Un approccio all'utilizzo di internet nella realtà lavorativa che sia coerente con il rispetto dei diritti umani, impone al datore di lavoro di adottare un quadro regolamentare interno trasparente concernente l'utilizzo della documentazione aziendale, di implementare coerentemente delle policy aziendali e di adottare eventuali misure di controllo proporzionate e non intrusive*".

3. *Outsourcers*

Il Garante ha recentemente analizzato il trattamento di dati personali effettuato da un partito politico italiano, la cui piattaforma *online*, utilizzata dagli elettori per votare il candidato di preferenza in occasione delle elezioni, è stata ripetutamente – e nel corso di un breve lasso temporale – esposta a *cyber* attacchi. Il provvedimento del Garante, pur dettato tenendo conto di una fattispecie particolare, ha ribadito alcuni principi generali. Più nello specifico, il provvedimento del Garante ha:

a) enfatizzato nuovamente il principio di trasparenza del trattamento (non solo da parte di un partito politico, ma da parte di qualunque titolare) e imposto di chiarire, all'interno dell'informativa *privacy* fornita agli interessati, il ruolo dei diversi soggetti coinvolti nel trattamento, ovvero:
   - titolari e contitolari del trattamento,
   - responsabili del trattamento (interni o esterni), soggetti alla supervisione del titolare, e
   - incaricati al trattamento, soggetti alla supervisione del responsabile e del titolare;

b) identificato un'illecita comunicazione di dati personali da parte del predetto partito politico, a favore di terzi fornitori di servizi esterni (che non erano stati indicati nell'ambito dell'informativa *privacy* agli iscritti); e, soprattutto,

c) prescritto un elenco di misure di sicurezza adeguate al fine di prevenire danni in caso di futuri *cyber* attacchi alla piattaforma *online*, quali:
   - il completamento di una valutazione di vulnerabilità,
   - il rafforzamento dei meccanismi di autenticazione degli utenti,
   - l'adozione di protocolli di comunicazione (http) più solidi e di algoritmi crittografati per tutelare le credenziali degli utenti, e
   - l'adozione di misure atte a monitorare le attività degli amministratori di sistema durante le sessioni di votazione *online*.

Dal provvedimento si possono trarre vari spunti di applicazione generale.

Il primo è che le società che trattano dati personali sono tenute a effettuare una revisione dei propri flussi di dati, al fine di assicurarsi che i destinatari di tali dati personali siano correttamente indicati nelle informative *privacy* fornite agli interessati, e che siano altresì ivi identificati quali responsabili del trattamento, o come contitolari dello stesso. Il secondo è che occorre implementare sistemi di sicurezza adeguati (protezioni IT) e svolgere quanto meno le attività sopra indicate sub (c).

Nuovi organismi (come il DPO), necessità di *policy* per i dipendenti e supervisione dei subfornitori: tutti aspetti rilevanti per la *privacy governance*. In effetti un approccio alla *privacy* che non tenga in considerazione la *governance* complessiva della società, si potrà ragionevolmente rivelare inefficace o, addirittura, controproducente. È, invece, necessario che la *privacy* (come l'anticorruzione) non sia considerata un mero adempimento formale, ma diventi parte integrante e fondamentale della *governance* aziendale e dell'organizzazione del *business*.

Newsletter FEBBRAIO 2018

Il Dipartimento di *Compliance* di Legance è a disposizione per qualsiasi chiarimento ed approfondimento, anche in relazione a fattispecie specifiche.

Per ulteriori informazioni:

Andrea Fedi

Partner

Tel. +39 06.93.18.271
afedi@legance.it

oppure il Vostro professionista di riferimento all'interno di Legance.

Newsletter FEBBRAIO 2018

LO STUDIO

Legance è uno studio legale italiano con un team di professionisti esperti, dinamici e orientati al risultato, il cui affiatamento ha reso possibile un modello organizzativo flessibile ed incisivo che, attraverso dipartimenti attivi in tutti i settori della consulenza legale d'affari, esprime il giusto equilibrio tra specialista e avvocato come consulente globale. Legance conta oltre 200 avvocati, nelle sedi di Milano, Roma, Londra e New York. Le aree di competenza sono: Fusioni, Acquisizioni e Diritto Societario; Banking; Project Financing; Debt Capital Markets; Equity Capital Markets; Financial Intermediaries Regulation; Fondi di Investimento; Contenzioso, Arbitrati ed ADR; Ristrutturazioni e Procedure Concorsuali; Ue, Antitrust e Regolamentazione; Diritto del Lavoro e delle Relazioni Industriali; Diritto Tributario; Diritto Amministrativo; Diritto Immobiliare; Diritto dell'Energia, Gas e Risorse Naturali; Compliance; Diritto della Navigazione e dei Trasporti; Proprietà Intellettuale; TMT (Technology, Media, Telecommunications); Diritto Ambientale; Insurance; Nuove Tecnologie; Legislazione Alimentare. Per maggiori informazioni, potete visitare il nostro sito web: www.legance.it.