Gli Approfondimenti della
Fondazione Studi Consulenti del Lavoro
Consiglio Nazionale dell'Ordine

APPROFONDIMENTO DEL 02/05/2018

GUIDA ALL'UTILIZZO DELLE NUOVE REGOLE IN MATERIA DI PRIVACY

PREMESSA

Dal 25 maggio trova piena applicazione la nuova normativa in materia di privacy che, come previsto dall'art. 99 del Regolamento UE 2016/679, è obbligatoria in tutti i suoi elementi e abroga espressamente la direttiva 95/46/CE.

Il presente vademecum si rivolge ai Consulenti del Lavoro con l'obiettivo di indicare le novità più significative in relazione agli adempimenti necessari ai fini del rispetto della normativa in materia di trattamento dei dati personali, alla luce della applicazione del Regolamento UE 2016/679.

Le indicazioni contenute hanno valore indicativo, limitandosi a tracciare le regole basilari comuni previste nel Regolamento comunitario, che come tale è immediatamente e direttamente applicabile nonché imperativo per gli Stati membri ed i singoli cittadini.

La natura non tassativa delle indicazioni tracciate è peraltro fisiologica conseguenza dell'essenza stessa del Regolamento, fondato sul principio della accountability, in virtù del quale è il titolare del trattamento ad essere investito del compito (e della responsabilità) di garantire l'adempimento agli obblighi previsti dalle norme e l'efficacia della tutela predisposta, in un bilanciamento di discrezionalità di adempimenti e responsabilità per la verifica della loro efficacia. Obblighi che comprendono quelli di riesame ed aggiornamento costante di tutte le condizioni adottate nel proprio sistema di trattamento e protezione dei dati personali.

LA DISCIPLINA

Trattamento dei dati personali (art. 5)

Ai sensi dell'art. 5 del Regolamento i dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le finalità devono essere determinate, esplicite e legittime.

Anche i dati trattati devono essere adeguati, circoscritti e limitati tenendo conto della necessità e della finalità. Al trattamento deve essere garantita adeguata sicurezza.

La trasparenza implica che ai titolari dei dati deve essere garantita l'informazione, chiara, semplice e facilmente accessibile, delle modalità attraverso le quali avviene l'utilizzazione, la consultazione e il trattamento dei dati personali che li riguardano.

Del rispetto dei princìpi fissati dall'art. 5, della loro adeguatezza, aggiornamento e sicurezza è responsabile il titolare del trattamento.

Liceità del trattamento e consenso (art. 6)

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. n. 196/2003.

Elemento fondamentale della liceità del trattamento è il consenso.

Consenso (art. 7)

Ai sensi dell'art. 7 del Regolamento il consenso deve essere prestato in maniera chiara e semplice, in forma comprensibile e facilmente accessibile.

Il Regolamento non prevede obbligatoriamente la forma scritta per il consenso. Tuttavia considerato che il titolare del trattamento, sempre ai sensi dell'art. 7, par. 1, è onerato di *"dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali"*, è evidentemente raccomandata l'opportunità di provvedere all'acquisizione del consenso in forma scritta.

Deve essere chiaro anche il riconoscimento del diritto a revocare il proprio consenso in qualsiasi momento.

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutti i requisiti indicati nel Regolamento (UE) 2016/679. In caso contrario è opportuno, prima di tale data, raccogliere nuovamente il consenso degli interessati secondo quanto previsto dalla novella normativa.

Consenso Obbligatorio

La prestazione del consenso deve essere tale da consentire la dimostrazione dell'effettività dei princìpi fissati dall'art. 7, rendendo chiaro ed inequivocabile:

a) che l'interessato ha acconsentito al trattamento;
b) che l'interessato ha prestato il consenso nella piena consapevolezza della misura e delle modalità con le quali il trattamento avviene;
c) forma accessibile e linguaggio semplice ed inequivocabile;
d) l'indicazione dell'identità del titolare del trattamento dei dati;
e) la finalità del trattamento cui sono destinati i dati personali;
f) la specifica indicazione del diritto alla revoca del consenso;
g) la separazione tra i consensi prestati rispetto ai dati ed alle finalità di trattamento, laddove distinti.

Consenso facoltativo

Il trattamento è considerato lecito quando è necessario:

- nell'ambito di un contratto o ai fini della sua conclusione o esecuzione;
- per adempiere ad un obbligo legale;
- per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Ricorrendo una delle precedenti ipotesi, il consenso non è necessario ed è sufficiente la consegna dell'informativa (con ricevuta che attesti la presa visione da parte dell'interessato), che conferma così la centralità e fondamentalità della propria funzione nell'ambito del trattamento dei dati personali. Si ricade in queste condizioni ed il trattamento dei dati – previa informativa – è lecito a prescindere dal consenso quando, ad esempio, i dati debbono essere acquisiti e trattati nell'ambito della gestione di un contratto e conseguente rapporto di lavoro, mandato professionale ed ogni attività fisiologicamente connessa (a mero titolo esemplificativo e non esaustivo: instaurazione e gestione del rapporto di lavoro; elaborazione prospetti paga; adempimenti dichiarativi in materia contributiva e fiscale; gestione di infortuni e malattia, etc.)

Categorie particolari di dati (art. 9)

Così come indicato all'art. 9 del Regolamento, il consenso all'acquisizione dei dati sensibili deve essere esplicito. Lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

Per espressa previsione dell'art. 9, par. 2, lett. b) del Regolamento, il divieto al trattamento, altrimenti previsto per i dati c.d. "sensibili", non si applica ed il trattamento è considerato lecito quando è necessario per assolvere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

Informativa (artt. 12 – 14)

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Il Regolamento non prevede una specifica forma di informativa, sebbene disponga che le informazioni di cui agli artt. 12 e seguenti debbano essere fornite per iscritto o anche in forma elettronica. Non è esclusa la forma orale, su richiesta dall'interessato, dovendo però comprovare l'identità di quest'ultimo.

Gli artt. 13 e 14 del Regolamento indicano le informazioni che devono essere fornite qualora i dati siano raccolti presso l'interessato (art. 13) o presso altri soggetti (art. 14).

L'informativa è un momento fondamentale del trattamento dati, ne caratterizza la fase iniziale ed accompagna ogni sua fase. Assolve in concreto al principio di trasparenza effettiva, garantendo all'interessato la possibilità di conoscere, ad esempio, il periodo di conservazione dei dati e le modalità tecniche attraverso le quali questa avviene. Il contenuto dell'informativa, complesso e più completo di quella già nota, deve essere utile a rendere edotto il titolare circa tutti i diritti che gli sono riconosciuti dal Regolamento, tra i quali necessariamente:

- diritto di accesso ai dati (art. 15);
- diritto di rettifica (art. 16);
- diritto alla cancellazione (c.d. "diritto all'oblio", art. 17);
- diritto di limitazione del trattamento (art. 18);
- diritto alla portabilità dei dati (art. 20);
- diritto di opposizione (art. 21).
-

Registri delle attività di trattamento (art. 30)

Il registro dei trattamenti (art. 30 Reg.) è uno strumento fondamentale ai fini del monitoraggio degli adempimenti e della garanzia dei diritti previsti dal Regolamento n. 2016/679.

La sua previsione non è obbligatoria per il titolare del trattamento che occupi meno di 250 dipendenti.

L'obbligo prescinde dal requisito dimensionale nel caso in cui i dati oggetto del trattamento possano presentare un rischio per i diritti e le libertà degli interessati, il trattamento non sia occasionale o includano dati sensibili, genetici, biometrici, giudiziari, così come individuati dagli artt. 9 e 10 del Regolamento.

Adeguatezza delle misure adottate (artt. 24 – 26)

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Ciò implica anche la verifica e l'eventuale necessità di adeguamento degli strumenti (*hardware* / software) attraverso i quali il trattamento viene effettuato.

Tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo, il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati (c.d. *"privacy by design"*).

Il titolare del trattamento attua misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi (c.d. *"privacy by default"*).

Valutazione d'impatto sulla protezione dati (artt. 35 – 36)

Sono obbligati alla valutazione d'impatto i titolari che debbano iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche, per le caratteristiche del trattamento o degli strumenti adottati per esso (ad esempio novità tecnologiche, finalità, natura dei dati).

Quando la valutazione di impatto indica che il trattamento presenta un rischio elevato, prima di procedere al trattamento, il titolare è tenuto a consultare l'autorità di controllo.

Al di fuori di tali esigenze specifiche non è un adempimento standard riferibile all'attività di consulenza del lavoro.

Nomina responsabili esterni (art. 28)

Qualora un trattamento debba essere effettuato per conto del titolare, quest'ultimo ricorre unicamente a responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il citato trattamento soddisfi i requisiti del Regolamento (UE) e garantisca la tutela dei diritti dell'interessato (art.28).

Nomina autorizzati al trattamento

Pur non prevedendo espressamente la figura dell'incaricato del trattamento, il regolamento non ne esclude la presenza, in quanto fa riferimento a persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4 par. 10).

Tale figura è colui che effettua materialmente le operazioni di trattamento sui dati personali. Può essere solo una persona fisica e deve agire sotto la diretta autorità del titolare o del responsabile del trattamento.

Data Protection Officer (art. 37 ss.)

Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese "Data Protection Officer" – DPO) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679.

La normativa non prevede tassativi requisiti per rivestire il ruolo di DPO. Il responsabile della protezione dei dati è designato, infatti, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'art. 39 del medesimo Regolamento (UE).

Non è obbligatorio per lo studio del singolo professionista, in quanto le attività principali dello stesso non consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

Non esplicitamente esclusi da tale obbligo i professionisti che svolgono la professione in forma associata o STP, per i quali, perlomeno per le realtà più strutturate, la nomina è raccomandata, anche alla luce del principio di *"accountability"* che caratterizza il Regolamento.

Data breach (art. 35)

Tutti i titolari del trattamento devono notificare all'autorità di controllo le violazioni di dati personali senza ingiustificato ritardo e, dove possibile, entro 72 ore dal momento in cui ne sono venuti a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, dovrà essere corredata dei motivi del ritardo (art.33).

Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica, con un linguaggio semplice e chiaro, la violazione all'interessato senza ingiustificato ritardo (art.34).

Sanzioni

All'art. 83 del Regolamento, par. 2, sono indicati i criteri che le autorità di controllo devono utilizzare per valutare sia l'opportunità di irrogare una sanzione amministrativa sia l'importo della stessa. Tali sanzioni devono essere in ogni caso effettive, proporzionate e dissuasive. Quasi tutti gli obblighi dei titolari e dei responsabili del trattamento sono classificati in base alla loro natura nelle disposizioni contenute all'articolo 83, paragrafi 4, 5 e 6. Il regolamento non fissa un importo specifico per ogni singola violazione, ma solo un massimale. Infatti, la violazione delle citate disposizioni è soggetta, a seconda delle diverse tipologie, a sanzioni amministrative pecuniarie fino a 10 o 20 milioni di euro o, per le imprese, fino al 2% o 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI
REGOLAMENTO (UE) 2016/679

Il sottoscritto_____

nato a_____ il_____

C.F._____

Residente a_____ Via_____ n._____

Tel._____ e-mail_____

Essendo stato informato:

☐ dell'identità del titolare del trattamento dei dati
☐ dell'identità del Responsabile della protezione dei dati
☐ della misura, modalità con le quali il trattamento avviene
☐ delle finalità del trattamento cui sono destinati i dati personali
☐ del diritto alla revoca del consenso

Così come indicato dalle lettere a, b, c, d, e, f dell'informativa sottoscritta ai sensi dell'art. 13 del Regolamento (UE) 2016/679

ACCONSENTE

ai sensi e per gli effetti dell'art. 7 e ss. del Regolamento (UE) 2016/679, con la sottoscrizione del presente modulo, al trattamento dei dati personali secondo le modalità e nei limiti di cui all'informativa allegata.

Letto, confermato e sottoscritto

_____, Li _____

_____
Firma del dichiarante (per esteso e leggibile)