Ordine dei Dottori Commercialisti ed Esperti Contabili di PESCARA

LINEE GUIDA IN MATERIA DI PRIVACY E PROTEZIONE DEI DATI PERSONALI
Maggio 2018

1. Premesse

L'Ordine dei Dottori Commercialisti ed Esperti Contabili di Pescara (di seguito, per brevità "ORDINE") adotta il presente Regolamento - suscettibile di costante aggiornamento – al fine di conformarsi alle disposizioni in materia di Privacy e protezione dei dati personali previste dal *General Data Protection Regulation*, ovvero Regolamento UE 679/2016 (di seguito, per brevità "GDPR" o "Regolamento UE"), applicabile a partire dal 25 maggio 2018.

L'ORDINE garantisce che i trattamenti dei dati personali si svolgano nel rispetto dei diritti e delle libertà fondamentali dell'interessato e della normativa in materia, sensibilizzando in tal senso tutti i membri del personale.

La nuova normativa privacy alla luce del Regolamento UE 679/2016

Il GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi, è volto ad armonizzare tutte le normative in materia di Privacy presenti all'interno dell'Unione Europea.

Il Regolamento UE muta l'approccio al tema della protezione dei dati personali, rafforzando ed incrementando la tutela dei diritti dell'interessato ed affidando un ruolo pro-attivo al Titolare ed al Responsabile del trattamento, accrescendone così la cd. *accountability*.

Inoltre, il Regolamento UE mira a focalizzare l'attenzione di tutte le figure coinvolte sul rispetto e sulla conformità dei trattamenti effettuati alla normativa europea, mediante:

- la cooperazione con le Autorità;

- l'incoraggiamento di meccanismi di certificazione;
- l'ampliamento del sistema di vigilanza;
- il rafforzamento del sistema sanzionatorio.

Quanto all'ambito di applicazione, il GDPR supera il principio della territorialità e si applica a tutti i trattamenti di dati personali da parte di Titolari non necessariamente stabiliti nell'Unione Europea, purché questi riguardino beni, servizi o comportamenti degli interessati all'interno dell'UE.

2. Principi del Trattamento

Il trattamento dei dati personali da parte dell'ORDINE è effettuato nel rispetto dei principi di cui all'art. 5 GDPR e, nello specifico:

- liceità, correttezza e trasparenza nei confronti dell'interessato;
- limitazione della finalità del trattamento;
- minimizzazione della raccolta dei dati;
- esattezza dei dati rispetto alle finalità per le quali vengono trattati;
- limitazione temporale della conservazione dei dati;
- integrità e riservatezza;
- responsabilizzazione del titolare.

3. Definizioni

Ai fini di una agevole comprensione del presente Regolamento, si riportano alcune delle definizioni contenute nell'art. 4 del Regolamento UE:

- "*dato personale*": qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- "*trattamento*": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione

mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- "*titolare del trattamento*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento dei dati personali;
- "*responsabile del trattamento*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare;
- "*destinatario*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi; (non sono considerati destinatari quelle autorità pubbliche che possono ricevere comunicazioni nell'ambito di una specifica indagine conformemente al diritto dell'Unione Europea).
- "*autorità di controllo*": l'autorità pubblica indipendente istituita da uno stato membro ai sensi dell'art. 51 GDPR
- "*profilazione*": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la saluta, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- "*pseudonimizzazione*": il trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, purché le medesime siano conservate separatamente e soggette a misure tecniche e organizzative tali da assicurare che i dati non siano attribuiti ad una persona fisica identificata o identificabile;
- "*consenso dell'interessato*": qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- "*violazione dei dati personali*": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

4. Tipologia trattamenti

Sono individuate le seguenti tipologie di trattamento:

- gestione anagrafica iscritti;
- gestione e tutela dell'Albo, dei registri e degli elenchi;
- organizzazione e gestione degli Esami di Stato;
- gestione dei dati in materia disciplinare (ricorsi/reclami);
- gestione dei dati in materia elettorale e dei membri degli organi elettivi;
- attività di formazione sia obbligatoria che facoltativa degli iscritti e gestione delle iscrizioni;
- gestione dei compensi e contratti dei dipendenti, consulenti e fornitori;
- gestione del contenzioso giudiziale, stragiudiziale ed attività di consulenza;
- altri trattamenti strumentali alle attività istituzionali.

5. Finalità del trattamento

Con il presente Regolamento l'ORDINE garantisce che i trattamenti di cui al paragrafo che precede vengano effettuati per finalità strettamente connesse all'attività svolta dall'ORDINE stesso - nel rispetto dei diritti e delle libertà fondamentali degli iscritti – e, nello specifico per: motivi istituzionali, amministrativo-contabili, di ricerca, commerciali.

6. Banche dati

Per banca dati si intende il complesso organizzato di una o più unità, dislocate in uno o più siti. L'ORDINE, in particolare, utilizza banche dati di tipo cartaceo ed informatico, software gestionali.

7. I soggetti del trattamento

L'ORDINE individua quali soggetti coinvolti nel trattamento dei dati personali le figure di seguito riportate.

7.1 Titolare

Il Titolare del trattamento è l'ORDINE - in persona del Presidente pro tempore dell'Ordine - in quanto esercita un potere decisionale autonomo in merito alle finalità ed i mezzi del trattamento dei dati personali degli iscritti.

Ai sensi dell'art. 24 del GDPR il Titolare mette in atto le misure tecnico-organizzative adeguate per garantire la conformità del trattamento ai principi di cui al paragrafo 2 del presente Regolamento.

Il Titolare del trattamento tiene un registro di tutti i trattamenti svolti sotto la propria responsabilità, conformemente a quanto prescritto dall'art. 30 n. 1 del GDPR.

7.2 Contitolare

In relazione ai trattamenti di cui al paragrafo 4 del presente Regolamento, è Contitolare degli stessi - ai sensi dell'art. 26 GDPR – la Fondazione per la promozione della cultura professionale e dello sviluppo economico, in quanto essa determina congiuntamente all'ORDINE le finalità ed i mezzi dei trattamenti suddetti.

7.3 Responsabile del trattamento

Sono Responsabili esterni tutti i soggetti esterni all'ORDINE che effettuano trattamenti sulle banche dati dello stesso, per suo conto e nel suo interesse; qualora, invece, questi determini autonomamente le finalità ed i mezzi del trattamento, deve considerarsi titolare dei trattamenti in questione.

I trattamenti da parte del Responsabile (interno o esterno) del trattamento sono disciplinati, ai sensi dell'art. 28 GDPR, da un contratto o altro atto giuridico che individui la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, le responsabilità affidate al Responsabile, gli obblighi ed i diritti del Titolare.

7.4 Persone autorizzate al trattamento (ex "incaricati")

Ai sensi dell'art. 29 GDPR, il Titolare o il Responsabile del trattamento individua - con apposite nomine e quali persone autorizzate al trattamento medesimo - tutti i dipendenti, collaboratori, consulenti, *outsourcers* che intervengono, in relazione all'esercizio delle rispettive mansioni e competenze, nell'esecuzione dei trattamenti.

Le persone autorizzate al trattamento dei dati personali agiscono, dunque, sotto l'autorità del Responsabile o del Titolare del trattamento.

Il presente regolamento identifica quali persone autorizzate al trattamento:
il personale della Segreteria dell'Ordine.

7.5 Responsabile della Protezione dei Dati (Data Protection Officer, "DPO")

Nelle ipotesi di cui all'art. 37 n. 1 lettere a), b), c), del GDPR, il Titolare o il Responsabile del trattamento designano un Responsabile della Protezione dei dati con comprovate conoscenze in materia di privacy, i cui riferimenti sono comunicati all'autorità di controllo.

Il Responsabile della Protezione dei dati può essere un dipendente dell'ORDINE o un soggetto esterno nominato in virtù di un contratto di servizi.

Ai sensi dell'art. 39 GDPR, il DPO ha, tra gli altri, il compito di:

- informare e fornire consulenza al Titolare o al Responsabile del trattamento;
- sorvegliare l'osservanza della normativa in materia di protezione dei dati personali, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale dell'ORDINE che partecipa ai trattamenti;
- fornire pareri, se richiesti;
- cooperare con l'autorità di controllo.

8. Diritti dell'interessato

Il presente Regolamento riconosce l'esercizio da parte dell'interessato dei diritti di cui agli artt. 15-21 del GDPR e, nello specifico: il diritto di accesso ai dati, di rettifica ed il diritto alla cancellazione ("diritto all'oblio") degli stessi, il diritto di limitarne il trattamento, il diritto alla loro portabilità, nonché il diritto di opposizione al trattamento.

9. Sicurezza del trattamento

Il Titolare ed il Responsabile del trattamento garantiscono, ai sensi dell'art. 32 GDPR, un livello di sicurezza adeguato al rischio per i diritti e le libertà degli interessati, adottando misure tecnico-organizzative, fra le quali:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità, nonchè la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali ed, in generale, la manutenzione dei sistemi informatici;
- una procedura per testare regolarmente l'efficacia delle misure adottate per prevenire e/o fronteggiare i potenziali rischi del trattamento.

10. Il *Data Protection Impact Assessment (DPIA)*

Con la valutazione d'impatto sulla protezione dei dati personali - di cui all'art. 35 del GDPR – l'ORDINE, in qualità di Titolare del trattamento dei dati personali intende garantire il rispetto dei requisiti di *compliance* in materia di Privacy previsti dal Regolamento UE.

Essa è diretta a valutare l'impatto che potrebbe avere un trattamento sulla sfera personale degli interessati e ridurre rischi ad esso connessi.

L'aspetto più innovativo del GDPR, infatti, è il passaggio dalla centralità del dato alla centralità dell'individuo: il DPIA mira, pertanto, a determinare se i trattamenti che l'ORDINE effettua possano – ed in che termini – pregiudicare le libertà fondamentali, i diritti e la dignità dell'interessato.

Si tratta di un processo codificato e strutturato nelle seguenti fasi:

1) giustificazione della DPIA: ovvero le ragioni per cui l'ORDINE ritiene necessaria una valutazione di impatto sui dati personali che intende trattare;
2) definizione dei flussi informativi: ovvero delle categorie di dati oggetto di trattamento, degli utilizzatori, delle sorgenti e dei destinatari finali del dato;
3) identificazione dei rischi: individuazione - in termini di probabilità e gravità - delle minacce che potrebbero concretizzarsi procurando un danno all'interessato;
4) selezione e valutazione delle soluzioni: al fine di ridurre il rischio ad un livello cd. accettabile;
5) *report* DPIA ed integrazione dei risultati.

Alla luce delle Linee Guida adottate nell'aprile 2017 dal Gruppo di lavoro articolo 29 - organo consultivo indipendente dell'UE per la protezione dei dati personali - e nel rispetto della disposizione di cui all'art. 35 co. 3 Regolamento UE, l'ORDINE effettua la valutazione d'impatto per trattamenti su larga scala che incidano su un vasto numero di interessati e che comportino un elevato rischio connesso *i)* all'introduzione di nuove tecnologie, *ii)* all'implementazione di trattamenti di profilazione o di sorveglianza o *iii)* all'utilizzo di particolari categorie di dati.

Ai sensi dell'art. 35 co. 7 del Regolamento UE, la valutazione di impatto effettuata dall'ORDINE prevede:

- una descrizione sistematica dei trattamenti previsti, delle finalità e l'eventuale ricorrenza di un interesse legittimo perseguito dal titolare;
- una valutazione della necessità e della proporzionalità dei trattamenti rispetto alle predefinite finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure organizzative e tecniche ed ogni meccanismo ritenuto utile per la tutela dei diritti degli interessati.

La responsabilità del processo di DPIA rimane in capo al Titolare del trattamento, il quale - all'occorrenza - potrebbe coinvolgere anche i responsabili aziendali, i responsabili esterni, i consulenti, gli *outsourcers*.

11. Consenso dell'interessato

Ogni qualvolta il trattamento dei dati personali richieda il consenso dell'interessato, tale consenso dovrà essere conservato e registrato.

L'interessato deve poter conoscere le modalità per prestare il consenso ed ha diritto - ogni qualvolta lo stesso venga richiesto ai fini del trattamento – di revocarlo in qualsiasi momento.

Laddove la raccolta di dati personali si riferisca a un minore di età inferiore ai 16 anni, il Responsabile della Protezione dei Dati deve garantire che il consenso dell'esercente la responsabilità genitoriale sia fornito prima della raccolta.

12. Informativa privacy

Ai sensi degli artt. 13 e 14 GDPR, il Titolare del trattamento fornisce all'interessato informazioni specifiche, chiare e sintetiche - sia nel caso di dati raccolti presso l'interessato che di dati raccolti presso terzi - sui trattamenti che intende effettuare.

13. Notifica di una violazione dei dati personali all'autorità di controllo

Il Titolare del trattamento è tenuto a notificare, secondo le modalità di cui all'art. 33 n. 3 GDPR, l'eventuale violazione dei dati personali – di cui sia venuto a conoscenza direttamente o su informazione del Responsabile del trattamento - all'autorità di controllo competente *ex* art. 55 del Regolamento UE, salvo che il rischio venga valutato come improbabile per i diritti e le libertà dell'interessato.

Ad ogni modo il Titolare, nel rispetto del principio di *accountability*, documenta qualsiasi violazione, così da consentire all'autorità di controllo di verificare la conformità del trattamento alla normativa vigente.

14. Comunicazione di una violazione all'interessato e trasparenza

Il Titolare del trattamento, altresì, comunica la violazione di dati personali all'interessato, qualora questa presenti rischi elevati per i diritti e le libertà dello stesso e salvo che non ricorrano le condizioni di cui all'art. 34 n. 3 GDPR.

La comunicazione può essere contestuale alla notifica di cui al paragrafo che precede e deve contenere, almeno, le seguenti informazioni:

- contatti del Responsabile della Protezione dei dati personali;
- probabili conseguenze della violazione in questione;
- le misure adottate o da adottare da parte del Titolare del trattamento per porre rimedio alla violazione.

15. Sanzioni

Il mancato rispetto delle disposizioni in materia di protezione dei dati personali è punito con l'applicazione di sanzioni amministrative pecuniarie, inflitte secondo i criteri di cui all'art. 83 GDPR ed, in generale, tenuto conto della natura della gravità e della durata della violazione, delle finalità del trattamento, del numero degli interessati lesi, del livello del danno e dell'aspetto doloso o colposo della violazione.

Resta ferma l'applicabilità di sanzioni penali, conformemente a quanto previsto dalla legislazione nazionale in materia.

16. Disposizioni finali

Per quanto non espressamente previsto nelle presenti Linee Guida, si applicano le disposizioni del Regolamento (UE) 2016/679 e dei provvedimenti del Garante per la protezione dei dati personali.