FNOVI
FEDERAZIONE NAZIONALE
ORDINI VETERINARI ITALIANI

Roma, 16 maggio 2018

Prot. n. 2567/2018/F/mgt
Circolare n. 4/2018

Ai Presidenti
degli Ordini Provinciali dei Veterinari

L O R O S E D I

Ai Componenti il Comitato Centrale
FNOVI
e il Collegio dei Revisori dei Conti

L O R O S E D I

Via e-mail - PEC

Oggetto: Regolamento UE 2016/679 in materia di protezione dei dati personali e Ordini professionali – Prime indicazioni per l'applicazione

Gentile Presidente,

in vista della scadenza del 25 maggio 2018 - che impone l'adeguamento al Regolamento UE 2016/679 sulla protezione dei dati personali (meglio noto come Regolamento Privacy, o con l'acronimo GDPR per eneral Data Protection Regulation) - gli Ordini professionali sono chiamati ad implementare presidi e misure organizzative finalizzate a ricevere e gestire i dati necessari da inserire negli Albi, a diffondere le relative informazioni, a rispondere agli accessi documentali e civici pervenuti da terzi, a gestire la pubblicità delle sanzioni disciplinari ed al contempo a tutelare i diritti degli iscritti.

Per quanto il quadro normativo non sia ancora completamente definito (non è stato ancora adottato il decreto legislativo per adeguare il quadro normativo nazionale alle disposizioni del Regolamento UE 2016/679 - GDPR) appare utile richiamare l'attenzione sulle principali novità legate all'applicazione del Regolamento Privacy e che riguardano:

- l'individuazione dei principali soggetti protagonisti del trattamento dei dati (il titolare del trattamento ed il responsabile del trattamento) nonché le caratteristiche dell'atto con cui il 'titolare' designa un 'responsabile del trattamento' attribuendogli specifici compiti;

- la designazione di un Responsabile della Protezione dei Dati (RPD – o Data Protection Officer - DPO)

- l'istituzione del registro dei trattamenti;

- la notifica di eventuali data breach;

- l'informativa.

* * * * * * * * * * * *

Titolare del trattamento e Responsabile del trattamento

Il Regolamento Privacy definisce le caratteristiche soggettive e le responsabilità del 'titolare del trattamento' e del 'responsabile del trattamento'.
Nel settore pubblico al quale afferiscono gli Ordini professionali, il titolare del trattamento, il soggetto che determina le finalità e gli strumenti del trattamento di dati personali, è l'Ente nel suo complesso. Quindi una persona giuridica anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno quali ad esempio, il Presidente dell'Ordine.
Il responsabile del trattamento è il soggetto che tratta dati personali per conto del titolare del trattamento. Potrà essere tanto una figura esterna quanto interna all'Ente e, in questo caso, la scrivente Federazione ritiene che il Consigliere con funzioni di "Segretario" possa essere il soggetto più idoneo da nominare[1].
La tutela dei dati personali disciplinata dal Regolamento Privacy si caratterizza per un approccio basato sul rischio, e consegna la protezione dei dati nelle mani del titolare, il quale, grazie al principio di responsabilizzazione ("*accountability*" [2].) potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presiedono il trattamento (lecito) dei dati personali.
Tale nuovo impianto tocca anche il ruolo del responsabile del trattamento, il quale è insignito di nuovi compiti, condivide in certa misura le responsabilità del titolare in ordine al risarcimento del danno a terzi, ed è oggetto di autonome sanzioni amministrative, a differenza di quanto avveniva con il Codice Privacy, ove la sanzione amministrativa era sempre diretta contro il titolare.

---

[1] A questo proposito, il Garante della Privacy, alla luce della disciplina interna aveva precisato che: "*è necessario precisare chi svolgerà l'eventuale ruolo di "responsabile del trattamento". Conseguentemente, l'Amministrazione deve decidere se prevedere tale figura ed attribuirne la responsabilità o alla struttura esterna cui è affidata l'attività in concessione, oppure ad un dipendente di quest'ultima, o a un proprio ufficio o dipendente dell'Amministrazione stessa (quest'ultima opzione presuppone che l'ufficio o il funzionario pubblico abbiano poteri effettivi di ingerenza sulle attività e sull'organizzazione dell'impresa concessionaria: cosa, in realtà, poco frequente). In concreto, la nomina del responsabile, che deve essere effettuata in forma scritta, potrebbe essere inserita in un apposito articolo della convenzione, oppure essere oggetto di un distinto provvedimento amministrativo o atto di diritto privato*".

[2] Il termine anglosassone non è facilmente traducibile e difatti nella traduzione del regolamento europeo si parla impropriamente di "responsabilità" mentre forse la traduzione più corretta, anche se poco pratica, potrebbe essere quella di "rendicontazione". L'accountability si compone di almeno tre elementi: 1. La "*trasparenza*" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio. 2. La "*responsività*" intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli stakeholder. 3. La "*compliance*" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori della PA.

La nomina a responsabile del trattamento è obbligatoria e non più facoltativa: il titolare e il responsabile regolano i loro rapporti contrattualmente. Il contratto tra titolare e responsabile del trattamento, oltre a vincolare a vicenda le due figure, deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.
All'art. 28 del Regolamento Privacy sono elencate nel dettaglio tutte le prescrizioni che tale contratto deve prevedere.
Per specifiche attività di trattamento, nel rispetto degli stessi obblighi che legano titolare e responsabile, è consentita la nomina - da parte del responsabile - di sub-responsabili del trattamento (art. 28, paragrafo 4 del regolamento); il responsabile del trattamento risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3).
Pur non prevedendo espressamente la figura dell'"incaricato" del trattamento (ex art. 30 Codice Privacy), 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*" (ove presenti, i collaboratori di segreteria dipendenti degli Ordini).

In allegato:

- *1. schema di atto per la nomina del 'responsabile del trattamento' ai sensi dell'art. 28 del Regolamento UE 2016/679 (soggetto interno all'Ordine)*
- *2. schema di accordo per la nomina del 'responsabile del trattamento' ai sensi dell'art. 28 del Regolamento UE 2016/679 (soggetto esterno all'Ordine)*

Il Responsabile della Protezione dei Dati (RPD)

L'Ordine, alla data del 25 maggio 2018, dovrà avere nominato il proprio Responsabile della Protezione dei Dati (RPD), interno o esterno: stante la natura di ente pubblico dell'Ordine, la sua designazione è obbligatoria.
Il Regolamento Privacy tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali) che non deve trovarsi in conflitto di interessi con il titolare del trattamento. In particolare il RPD – figura chiave del nuovo sistema di *governance* dei dati – non può rivestire, all'interno dell'Ordine, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali.
Nel caso in cui l'Ordine opti per un RPD interno, 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, nonché in contatto diretto con il vertice dell'organizzazione (art. 38). Non è possibile nominare RPD un Consigliere dell'Ordine ma la scrivente Federazione ritiene che un Revisore dei Conti possa essere coinvolto nell'incarico, al pari di un qualsiasi altro iscritto all'Ordine, purché versi in una situazione di totale indipendenza rispetto al Consiglio dell'Ordine stesso.
Se si opta per un RDP esterno bisogna seguire le regole del Codice dei contratti pubblici, ricordando che è ammesso l'affidamento dell'incarico mediante le procedure semplificate di cui all'articolo 36 del medesimo Codice, compreso l'affidamento diretto.
Il Regolamento ha inserito per i titolari del trattamento dei dati l'obbligo di comunicare al Garante la designazione del nuovo responsabile della protezione dei dati (RPD), con lo scopo di creare presso l'Autorità un elenco nazionale. La comunicazione, che si compone di quattro fogli, andrà compilata online accedendovi attraverso il sito del Garante

(www.garanteprivacy.it). Dopo aver inserite tutte le informazioni, si riceverà una mail con allegato un file, che dovrà essere sottoscritto con firma digitale qualificata del Presidente pro-tempore e rispedito entro 48 ore dalla ricezione. Se non ci sono irregolarità, chi ha effettuato la comunicazione riceverà il numero di protocollo della pratica e il titolare del trattamento nonché il RPD saranno informati dell'esito dell'operazione attraverso l'indirizzo PEC indicato nella comunicazione al Garante.

In allegato:

- *3. schema di atto di designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679*
- *4. Facsimile della Comunicazione al Garante dei dati del Responsabile della Protezione dei Dati personali (RDP)*

Il Registro dei trattamenti

L'Ordine professionale deve redigere e tenere aggiornato il Registro dei Trattamenti anche ai fini dell'eventuale supervisione e richiesta di esibizione da parte del Garante. Tale nuovo adempimento consente alle singole organizzazioni di rispondere a una pluralità di finalità, tra cui:

• tenere traccia delle operazioni di trattamento effettuate all'interno della singola organizzazione;

• costituire uno strumento operativo di lavoro mediante il quale censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un efficace 'ciclo di gestione' dei dati personali;

• dimostrare di aver adempiuto alle prescrizioni del Regolamento privacy, nell'ottica del principio di "*accountability*".

Si tratta in realtà di due registri che presentano delle differenze dal punto di vista contenutistico, avendo il primo (il registro dei trattamenti del titolare del trattamento ex art. 30, comma 1, del Regolamento UE 2016/679) una portata più ampia che si estende all'indicazione delle finalità del trattamento, delle categorie di interessati e delle categorie di dati personali, delle categorie di destinatari a cui i dati personali sono stati o saranno comunicati (compresi i destinatari di paesi terzi od organizzazioni internazionali), dei termini ultimi previsti per la cancellazione delle diverse categorie di dati (ove possibile). Il secondo (il registro dei trattamenti del 'responsabile del trattamento' ex art. 30, comma 2, del Regolamento UE 2016/679) registra tutte le categorie di attività relative al trattamento svolte per conto del 'titolare del trattamento'.

Non è disciplinata a livello normativo una regola generale che stabilisca le modalità attraverso le quali costruire il registro dei trattamenti: l'art. 30 del Regolamento Privacy, infatti, si limita ad indicare quali sono gli elementi che il registro deve necessariamente contenere ed in relazione alla tenuta del registro appare utile una elencazione, per quanto non esaustiva, dei dati trattati dall'Ordine.

I Consigli dell'Ordine sono titolari di dati personali: degli iscritti (dati personali e categorie particolari di dati come dati relativi alla salute art. 9 del Regolamento Privacy); dei consulenti; dei dipendenti; dei dati relativi ad atti amministrativi e fiscali; dei fornitori (persone fisiche); dei dati relativi agli esposti o alle denunce, o all'acquisizione di notizie di fatti suscettibili di valutazione disciplinare; dei dati relativi ai poteri di vigilanza, controllo e monitoraggio regolare e sistematico degli iscritti negli Albi professionali.

In allegato:

- *5. schema di registro dei trattamenti ai sensi dell'art. 30 del Regolamento UE 2016/679*

Data breach

L'art. 31 del Regolamento Privacy dispone che in caso di violazione dei dati personali, a partire dal 25 maggio 2018, il responsabile del trattamento deve notificare la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ingiustificato ritardo e cioè, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora non effettuata entro 72 ore, la notifica all'autorità di controllo dovrà corredarsi di una giustificazione motivata.

Informativa

Ciascun Ordine deve dare l'informativa prevista dagli articoli 13 e 14 del Regolamento Privacy. Si considera sufficiente la pubblicazione dell'informativa sul sito web e, nel contempo si afferma che non si ritiene necessaria l'informativa se la registrazione o la comunicazione dei dati personali sono previste per legge (come, ad esempio i dati degli Albi, elenchi e registri ex art. 15 L 247/2012 e D.M. Giustizia 16 agosto 2016 n.178).

In allegato:

- *6. schema di informativa*

* * * * * * * * * * * *

Nel precisare che i contenuti delle presente Circolare non possono essere considerati esaustivi delle previsioni di cui al Regolamento Privacy, ma forniscono solo una iniziale indicazione degli adempimenti da eseguire per l'avvio delle procedure necessarie per l'adeguamento alle nuove previsioni, si esprime riserva di tornare in argomento per fornire ogni ulteriore indicazione ritenuta utile (come ad esempio la redazione di "linee guida in materia di privacy e protezione dei dati personali" o la predisposizione di indicazioni fruibili dagli iscritti affinché verifichino autonomamente l'adeguatezza della propria organizzazione al Regolamento).

Si consiglia, nel frattempo, la consultazione di una pagina[3] che l'Autorità ha dedicato all'informazione sul Regolamento UE/2016/679, dove sono disponibili anche una guida per l'applicazione del Regolamento e vari documenti utili, come le Linee guida che il Garante ha contribuito a definire in sinergia con le altre Autorità privacy europee per facilitare la comprensione e l'applicazione del nuovo quadro normativo.

Con l'occasione si rammenta che, nel caso non fossero previste riunioni dei Consigli Direttivi entro la data del 25 maggio p.v., potranno adottarsi delibere presidenziali d'urgenza che saranno in seguito ratificate.

Ringraziando per l'attenzione e rammentando che gli Uffici FNOVI sono a disposizione per quanto altro possa occorrere, è gradita l'occasione per porgere un cordiale saluto.

Il Presidente
(Dott. Gaetano Penocchio)

Allegati

[3] Vedi al link https://www.youtube.com/playlist?list=PLVtg2nJEE4IMRjxAAkocBjVpx8-fIeidT