CONSIGLIO
DELL'ORDINE NAZIONALE
DEI DOTTORI AGRONOMI
E DEI DOTTORI FORESTALI

Protocollo Generale N.		Entrata	
		Uscita	2538
Data di Arrivo		Data di Partenza	14/05/2018
Responsabile di Protocollo			
Area Amministrativa		Area Giurisdizionale	
AA	Codice Categoria	AG	Codice Categoria
Area Amministrazione Contabilità			
AAC	Codice Cat.	N. Reg	
		Data Reg.	
Data di Pubblicazione			
Responsabile Pubblicazione			

Alla c.a.	Presidenti degli Ordini dei Dottori Agronomi e dei Dottori Forestali
sede	LORO SEDI
Alla c.a.	Presidenti delle Federazioni degli Ordini dei Dottori Agronomi e dei Dottori Forestali
sede	LORO SEDI
E p. c.	Consiglieri Nazionali
sede	LORO SEDI
	Coordinatore Centro Studi CONAF Dott. Giancarlo Quaglia
sede	LORO SEDI

Circolare	*Codice Atto*	*Numero*	*Anno*	*Autore*	*Estensore*
	AA1E	*18*	*2018*	*AS*	*bb*

Oggetto	***Informativa Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo ai dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).***

Gentili ed egregi colleghe/ghi,

il 25 maggio p.v. entrerà in vigore il nuovo Regolamento UE 679/2016 che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) e che riguarda la protezione delle persone fisiche con riguardo ai dati personali, nonché alla libera circolazione di tali dati.
Qui di seguito si riportano le parti più salienti del nuovo Regolamento che si allega alla presente (allegato 1).

1) AMBITO DI APPLICAZIONE

Gli ambiti dei applicazione **materiale e territoriale** del Regolamento UE 679/2016 sono regolati dagli artt. 2 e 3 del Regolamento UE 679/2016.

2) I SOGGETTI COINVOLTI

Con particolare riferimento agli Ordini Professionali, nell'ambito dei soggetti coinvolti nel trattamento dei dati regolato dal nuovo regolamento, vi sono, innanzitutto, l'Ordine, in quanto titolare del trattamento dei dati, in persona del Presidente.
Infatti, ai sensi dell'art. 4 n. 7 del Regolamento, è l'Ordine che determina in maniera autonoma finalità e mezzi del trattamento dei dati personali, nel caso specifico, degli iscritti.

Altri soggetti coinvolti nel trattamento sono:

a. interessato;
b. il titolare del trattamento;
c. responsabile del trattamento;
d. il contitolare del trattamento;
e. le persone autorizzate al trattamento;
f. il responsabile della protezione dei dati.

a) Interessato

Per *interessato* si intende la persona fisica cui si riferiscono i dati personali.

b) Titolare del trattamento

Il titolare del trattamento è 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, nel caso specifico il titolare del trattamento è l'Ordine, i persona del Presidente.
Ai sensi dell'art.24 del Regolamento UE 679/2016, il Titolare mette in atto le misure tecnico organizzative adeguate per garantire la conformità del trattamento ai principi di cui all'art.5 del Regolamento UE 679/2016.

c) Responsabile del trattamento

Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare;

Al titolare del trattamento e al responsabile del trattamento è affidato un ruolo pro-attivo, dovendo – nel rispetto del più generale principio di responsabilizzazione ("accountability") – porre in essere e aggiornare tutte le misure tecniche e organizzative adeguate volte a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in maniera conforme al Regolamento (artt. 5 e 24 par. 1 del Regolamento).

I trattamenti svolti da parte del *responsabile del trattamento* – che può essere interno o esterno – sono disciplinati da un contratto o altro atto giuridico avente ad oggetto la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, le responsabilità affidate allo stesso responsabile, gli obblighi ed i diritti del titolare.
Il *titolare* deve impartire specifiche istruzioni al *responsabile del trattamento* ai fini del trattamento dei dati personali; in caso di trattamenti particolarmente complessi, il responsabile può nominare, a sua volta, un sub-responsabile.

Il responsabile del trattamento esterno sono tutti quei soggetti esterni all'Ordine che effettuano trattamenti sulle banche dati dello steso, 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.

Il Responsabile, interno o esterno del trattamento tiene, al pari del Titolare, il registro delle attività di cui all'art.30 n.2 del Regolamento UE 676/2016, svolte per conto del Titolare stesso. Il

Responsabile del trattamento deve trattare i dati personali secondo le direttive impartitegli dal Titolare ed in caso di necessità può nominare, a sua volta un ***sub-responsabile***.

d) Persone autorizzate al trattamento

Accanto al *titolare del trattamento* (e *al responsabile*) vi sono le figure delle persone autorizzate al trattamento, che agiscono – dietro apposita nomina – sotto l'autorità dello stesso.
In concreto, si tratta di tutti quei soggetti, quali dipendenti, collaboratori, consulenti e outsourcers, che intervengono nell'esecuzione dei trattamenti rispetto alle proprie mansioni e competenze (art. 29 del Regolamento).

e) Contitolare del trattamento

Accanto all'Ordine può essere previsto un *contitolare del trattamento*, qualora le finalità ed i mezzi dei trattamenti siano determinati congiuntamente (art. 26 del Regolamento UE 679/2016).
Mediante uno specifico accordo sono disciplinate anche le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti degli interessati e ai ruoli per la comunicazione dell'informativa.

In considerazione, della molteplicità delle funzioni dell'Ordine, il CONAF ha predisposto anche due modelli (allegati 6 e 7) relativi alla designazione dei responsabili del trattamento (art. 28 del Regolamento), definiti dall'art. 4 n. 8 del Regolamento come i soggetti che trattano dati personali per conto del titolare del trattamento.
Si precisa che, qualora il responsabile del trattamento determini in maniera autonoma finalità e mezzi del trattamento, è considerato direttamente un titolare del trattamento in questione.

Infine, va menzionata anche la nomina, nei casi di cui all'art. 37 par. 1 del Regolamento, del Responsabile della protezione dei dati (RPD), che può essere un dipendente dell'Ordine o un soggetto esterno nominato in forza di un contratto di servizi.

f) Responsabile della protezione dei dati (Data Protection Officer, "DPO")

Gli artt. 37, 38 e 39 del Regolamento UE 679/2016 regolano la designazione, posizione e compiti del **Responsabile della protezione dei dati (DPO).**
La designazione del DPO avviene nelle ipotesi di cui all'art.37 n.1 lettere a), b), c) del Regolamento UE 679/2016, per cui il Titolare o il Responsabile del Trattamento designano un Responsabile della protezione dei dati con comprovata conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.
Il DPO può essere un dipendente del Titolare del trattamento o assolvere i suoi compiti in base a un contratto di servizi.
Il Titolare del trattamento o il Responsabile del trattamento pubblica i dati di contatto del responsabile dei dati e li comunica all'autorità di controllo.

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.

3) TIPOLOGIE DI TRATTAMENTO DEGLI ORDINI PROFESSIONALI

Fra le tipologie di trattamento che maggiormente interessano l'Ordine, in particolare, vi sono:

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

L'Ordine, poi, effettua, secondo quanto prescritto dall'art.35 par.3 del Regolamento, una **valutazione d'impatto sulla protezione dei dati (DPIA)** per i trattamenti su larga scala che incidono su un vasto numero di interessati e che comportano un elevato rischio connesso, fra l'altro, all'utilizzo di particolari categorie di dati.
L'Ordine deve anche garantire un livello di sicurezza adeguata al rischio per i diritti e le libertà degli interessati, adottando determinate **misure tecnico-organizzative**, quali, ad esempio, la pseudonimizzazione (art.4, comma 5) e la cifratura dei dati personali (art. 32 par. 1 del Regolamento).

La liceità del trattamento è regolata dall'art.6 capo II del Regolamento UE 679/2016.

4) IL REGISTRO DEI TRATTAMENTI

Tra le novità introdotte dal Regolamento Ue, vi è poi **il registro delle attività di trattamento**, strumento per il monitoraggio degli adempimenti ed in cui il Titolare del trattamento (cioè l'Ordine nella persona del Presidente) , fra gli adempimenti privacy, è tenuto a compilare di tutti i trattamenti svolti sotto la propria responsabilità (art. 30 par. 1 del Regolamento UE 679/2016).

Tale registro non è obbligatorio per i titolari del trattamento che stiano entro determinati limiti dimensionali (250 dipendenti), a meno che:

- i dati oggetto del trattamento presentino un rischio per i diritti e le libertà degli interessati;
- il trattamento non sia occasionale o includa i dati sensibili individuati dagli artt. 9 e 10 del regolamento.

5) FINALITA' DEL TRATTAMENTO

Con il presente regolamento l'Ordine garantisce che i trattamenti di cui al punto 3 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 etc…

6) BANCHE DATI

Con **base di dati** o **banca dati** si indica un insieme di dati, omogeneo per contenuti e per formato, memorizzati in un elaboratore elettronico e interrogabili via terminale utilizzando le chiavi di accesso previste (siti internet, software gestionali, elenchi elettronici locali etc.), ma anche gli archivi cartacei.

7) 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:

a. la pseudonimizzazione (art.4, comma 5) e la cifratura dei dati personali;
b. la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità, nonchè la resilienza dei sistemi e dei servizi di trattamento;
c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali ed, in generale, la manutenzione dei sistemi informatici;
d. una procedura per testare regolarmente l'efficacia delle misure adottate per prevenire e/o fronteggiare i potenziali rischi del trattamento.

8) DIRITTI DELL'INTERESSATO

I diritti dell'Interessato al trattamento dei dati sono regolati dal CAPO III del Regolamento UE 679/2016 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 portabilità, nonché il diritto di opposizione al trattamento.

9) CONSENSO DELL'INTERESSATO

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

Secondo il Regolamento in esame, i dati dovranno essere trattati in modo *lecito, corretto e trasparente* nei confronti dell'interessato e le finalità del trattamento dovranno essere *determinate, esplicite e legittime.*
In particolare, la trasparenza implica che ai titolari dei dati debba 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.
Il regolamento definisce il consenso al trattamento dei dati come un elemento fondamentale della liceità del trattamento. Questo può essere obbligatorio o facoltativo (ad esempio quando i dati sono trattati nell'ambito di un contratto di lavoro), per cui è sufficiente la consegna dell'informativa con ricevuta di presa visione da parte dell'interessato.
Il consenso deve essere prestato in maniera chiara, semplice, comprensibile e facilmente accessibile e dev'essere ben chiaro il riconoscimento del diritto a revocarlo. Inoltre, nonostante non vi sia l'obbligo di forma scritta, il titolare del trattamento, ai sensi dell'art. 7, comma 1 del Regolamento UE 679/2016, ha l'onere di "dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali".

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.

Per quanto riguarda l'informativa, che caratterizza la fase iniziale e accompagna ogni fase del trattamento, quest'ultima deve contenere tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, e permettere al titolare la conoscenza di tutti i diritti che gli sono riconosciuti dalla normativa (tra cui il diritto di accesso ai dati, di rettifica e di limitazione del trattamento).

ATTENZIONE: I consensi prestati prima del 25 maggio 2018 restano validi solo se rispettano tutti i requisiti indicati nel Regolamento UE 679/2016.

10) INFORMATIVA PRIVACY

Ai sensi degli artt. 13 e 14 del Regolamento UE 679/2016, 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.

11) 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.

12) 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 del regolamento UE 679/2016.

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.

13) 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 del Regolamento UE 679/2016 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.

14) ORDINE PROFESSIONALE E RAPPORTI DI LAVORO

Nell'ambito dei contratti di lavoro degli Ordini si segnala come, per la nuova normativa, sia sufficiente l'informativa sulla privacy.
In vista della piena applicazione, dal prossimo 25 maggio, delle nuove regole in materia di Privacy in seguito all'entrata in vigore del Regolamento Ue n. 679/2016, anche la Fondazione studi del Consiglio nazionale dei consulenti del lavoro ha pubblicato una guida che si rivolge, in particolare, ai Consulenti del lavoro con l'obiettivo di indicare le novità più significative in materia di trattamento dei dati personali del personale dipendente.
Tali indicazioni ben si adattano alle peculiarità di tutti gli ordini e collegi delle professioni regolamentate.

15) IL DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Secondo quanto previsto dall'art.35 del Regolamento UE 679/2016, l'Ordine, in qualità di Titolare del trattamento dei dati personali, deve garantire il rispetto dei requisiti di *compliance* in materia di Privacy previsti dal Regolamento UE attraverso la **valutazione d'impatto sulla protezione dei dati personali (DPIA).**

Tale istituto è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo.

L'articolo 35, comma 1, del GDPR prevede che il processo di DPIA sia obbligatorio quando un trattamento di dati personali "presenti un rischio elevato per i diritti e le libertà delle persone fisiche". Sul punto, al fine di assicurare un'interpretazione coerente delle circostanze in cui risulta obbligatorio lo svolgimento di un DPIA, il gruppo di lavoro ex articolo 29 (gruppo di lavoro a cui fanno parte tutte le Authority Privacy di ciascun Stato Membro dell'Unione Europea c.d. "WP-29") ha pubblicato il 4 aprile 2017 un documento contenente le linee guida per lo svolgimento di un DPIA chiarendo il concetto espresso dal primo comma dell'articolo 35.
Il soggetto obbligato ad effettuare un DPIA è il titolare del trattamento con il supporto del DPO, se nominato, e del responsabile del trattamento eventualmente coinvolto.
Al titolare del trattamento spetta, quindi, di assicurare che il DPIA venga eseguita assumendosene l'intera responsabilità.
Il titolare del trattamento è tenuto a consultarsi con il DPO, qualora designato, e dovrà attenersi al parere ricevuto.
Il DPO dovrà monitorare lo svolgimento del DPIA e fornire il suo parere per iscritto che sarà determinante ai fini dell'esito positivo o meno del processo di DPIA.
Nello svolgimento del DPIA, il titolare del trattamento dovrà altresì raccogliere le opinioni degli interessati o dei loro rappresentanti.

Il regolamento UE 679/2016 definisce ed individua le caratteristiche minime per svolgere un processo di DPIA distinguendolo in varie fasi:

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

Si rammenta che la realizzazione di un DPIA costituisce un processo continuativo e non un esercizio una tantum in quanto è da considerarsi come uno strumento volto a contribuire al processo decisionale in materia di trattamento dei dati personali da parte di un titolare del trattamento e di un responsabile del trattamento.

16) MISURE TECNICHE E ORGANIZZATIVE ADEGUATE

Il titolare del trattamento dovrà anche mettere in atto misure tecniche e organizzative adeguate per garantire la conformità del trattamento alla normativa Ue (analizzate dal Garante della privacy), che devono essere al passo con il progresso tecnologico, in modo da garantire la tutela dei diritti degli interessati ("privacy by design") e il trattamento dei soli dati personali necessari per ciascuna finalità ("privacy by default").

Inoltre, il Garante della privacy, nel tutorial che agevola il titolare del trattamento ad individuare e gestire il rischio durante la valutazione dell'impatto, ha definito il rischio come "lo scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà dell'interessato". Pertanto, i titolari che devono intraprendere un trattamento rischioso per i diritti e le libertà delle persone fisiche, devono valutarne l'impatto tenendo conto di elementi quali l'origine, la natura, la gravità del rischio e, qualora questo sia troppo elevato, prima di procedere dovranno consultare l'autorità di controllo.

In caso di violazioni dei dati personali, tutti i titolari del trattamento, entro 72 ore dal momento in cui ne sono venuti a conoscenza o comunque senza ritardo, devono notificarle all'autorità e, nei soli casi in cui la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, anche all'interessato; in proposito, l'art. 83 del Regolamento Ue illustra i criteri che le autorità di controllo dovranno applicare nella valutazione circa l'opportunità di irrogare o meno una sanzione, che dovrà, in ogni caso, essere effettiva, proporzionata e dissuasiva.

CONSIGLIO
DELL'ORDINE NAZIONALE
DEI DOTTORI AGRONOMI
E DEI DOTTORI FORESTALI

Per presa visione di tutti gli adempimenti inerenti il nuovo regolamento sulla protezione dei dati si rimanda al *Regolamento UE 679/2016* in allegato alla presente.

Inoltre, in attuazione di quanto disposto dal Regolamento UE 679/2016 si inviano, in allegato, le linee guida in materia di privacy e protezione dei dati personali e alcuni modelli che dovranno essere adottati dagli Ordini territoriali entro la data del 25 maggio p.v., nel dettaglio:

- gli accordi di con titolarità sul trattamento dei dati personali (art. 26 del Regolamento);
- l'informativa per il trattamento dei dati personali in riferimento ai fornitori e agli utenti che consultano il sito web degli Ordini (artt. 13 e 14 del Regolamento);
- la designazione del Responsabile della protezione dei dati (art. 37 del Regolamento);
- la nomina dei responsabili del trattamento, interni o esterni (art. 28 del Regolamento).

Rimanendo a disposizione per qualsiasi chiarimento, porgiamo distinti saluti
Cordiali saluti

Il Presidente
Andrea Sisti, Dottore Agronomo

CONSIGLIO DELL'ORDINE DEI DOTTORI AGRONOMI E DOTTORI FORESTALI
Via Po, 22
ROMA

ALLEGATI:

1) Regolamento (UE) 2016-679 in materia di protezione dei dati personali.
2) Accordo di contitolarità, Fac simile.
3) Informativa Fornitori, Fac Simile.
4) Informativa Sito Web, Fac Simile.
5) Nomina DPO, Fac Simile.
6) Nomina responsabile esterno, Fac Simile.
7) Nomina responsabile interno, Fac Simile.