ASSEMBLEA ORDINE GEOLOGI PIEMONTE

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

principali adempimenti

17 maggio 2019 - Hotel Fortino Strada del Fortino n. 36 Torino

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Il Regolamento 679/2016

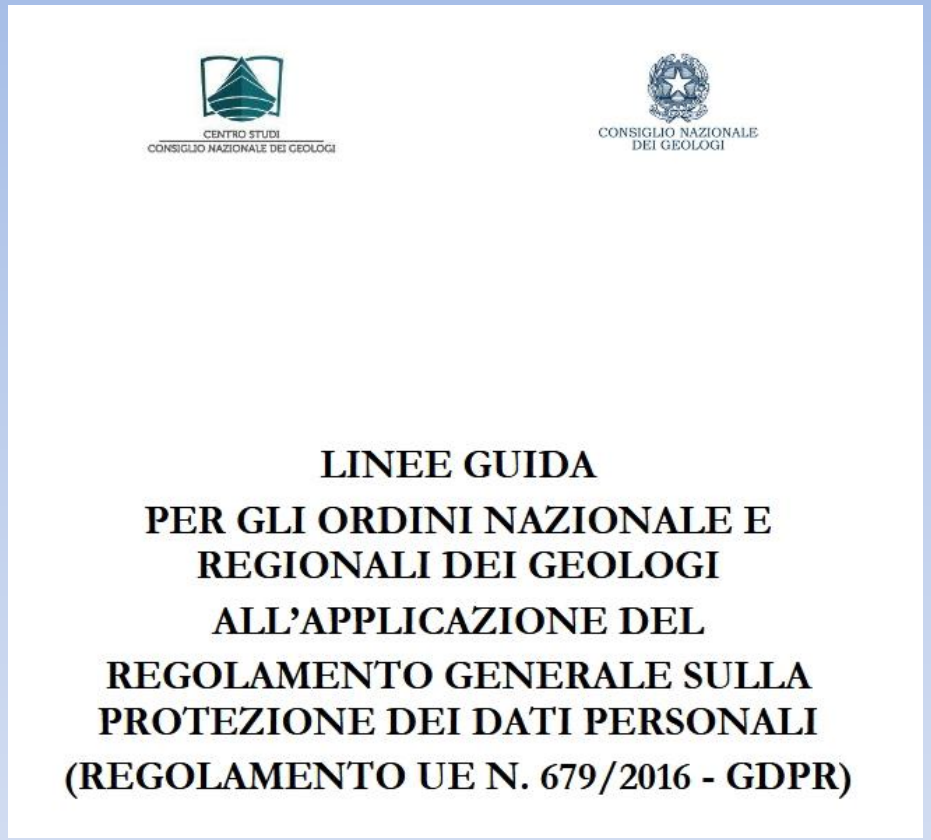
In vigore dal 25 maggio 2016

Si applica dal 25 maggio 2018

<u>Delibera Garante Privacy 14/02/19 con prospetto piano ispettivo 1^semestre</u>
(Istituti di credito, sanità, sistema statistico nazionale (Sistan), Spid, telemarketing, carte di fedeltà, grandi banche dati pubbliche)

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

E' fatto obbligo di uniformarsi al GDPR anche ai professionisti in quanto l'inadempienza comporta responsabilità **amministrative** e **penali** e **rafforza l'apparato sanzionatorio**



L'impatto del regolamento sull'attività dei professionisti

Il Regolamento pur con molte mediazioni **stabilisce nuovi diritti sul trattamento dei dati personal**i:

- si applica:

1. al trattamento dei dati personali delle persone fisiche
2. al trattamento automatizzato di dati personali
3. al trattamento non automatizzato di dati personali contenuti in un archivio

- Introduce nuove regole organizzative per il corretto trattamento dei dati personali. **Non è più richiesto** il requisito del **consenso espresso** se non per le attività di profilazione
- Definisce sanzioni pesanti e commisurate al fatturato:

•Violazioni agli obblighi: fino a 10.000.000 per i privati e le imprese non facenti parte di gruppi, Fino al 2% del fatturato complessivo (consolidato) per i Gruppi societari

•Violazioni dei principi del regolamento e dei diritti degli interessati: fino a € 20.000.000 per i privati e le imprese non facenti parte di gruppi.

Fino al 4% del fatturato complessivo (consolidato) per i Gruppi societari

- Crea meccanismi di tracciabilità che imporranno al professionista di allocare nella struttura le responsabilità nel trattamento dei dati personali.

La gestione dei dati personali non sarà più solo un **adempimento**, ma diventa un **processo** che incide sull'organizzazione dell'attività professionale

DATO PERSONALE

•Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)

•Si considera identificabile la persona fisica che può essere identificata con particolare riferimento a un identificativo come il nome, dati relativi all'ubicazione, numero di telefono, indirizzo e-mail, identificativo online

•E' vietato trattare dati personali che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati relativi alla salute o alla vita sessuale se non tramite consenso esplicito o per motivi di interesse pubblico nei casi previsti dalla legge

TRATTAMENTO DEL DATO PERSONALE

si intende qualsiasi attività di gestione, come ad esempio:

- la raccolta
- la conservazione
- la modifica
- la comunicazione
- la cancellazione

su qualsiasi supporto

- informatico
- cartaceo

sia attraverso operatori sia con processi automatizzati

PRINCIPALI ADEMPIMENTI

La normativa responsabilizza il Professionista sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Tra le misure tecniche ed organizzative da adottare ricordiamo le principali:

- Mappatura dei processi e valutazione dei rischi connessi
- Adeguare i moduli informativi e di consenso verso gli interessati
- Nominare gli incaricati del Trattamento
- Redigere il Registro dei Trattamenti
- Raccogliere i consensi e conservarli in luogo adeguato, informaticamente: in modo tracciato/certo ed individuabile.
- Adottare le misure minime di sicurezza a livello di ICT
- Gestione delle violazioni entro 72 ore

PRINCIPALI ADEMPIMENTI

AGGIORNAMENTO MODULISTICA

effettuare l'aggiornamento della modulistica per committenti e fornitori

Sul sito dell'ORGP
(https://www.geologipiemonte.it/l-ordine/atti-circolari-pareri-orgp/articolo/nuovo-regolamento-sulla-privacy-gdpr-679-2016-in-vigore-dal-25-ma)

È consultabile/scaricabile il fac-simile per

- Studio singolo
- Studio associato

PRINCIPALI ADEMPIMENTI

NOMINA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

La nomina del RPD è prevista qualora si effettui trattamento di dati personali su larga scala rientrando nelle previsioni dell'art. 37, co. 1, lett. c) del GDPR: "*Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9* (ex dati c.d. "sensibili" ora "dati particolari") *o di dati relativi a condanne penali e a reati di cui all'articolo 10*".

Qualora non rientri nella casistica precedente, il singolo professionista non è tenuto a nominare un RPD

PRINCIPALI ADEMPIMENTI

REGISTRO ATTIVITA' DI TRATTAMENTO (art. 30 del GDPR)

L'istituzione del registro delle attività di trattamento svolte e le procedure adottate sotto la propria responsabilità per la sicurezza.

Il comma 5 del medesimo regolamento indica però che "*gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*".

Qualora non rientri nella casistica precedente, il singolo professionista non è tenuto ad istituire il registro attività

Per completezza di informazione si rende noto che il Garante della Privacy consiglia comunque l'istituzione e l'aggiornamento del Registro in quanto strumento assai utile per la diagnosi e valutazione dei dati trattati dall'organizzazione

PRINCIPALI ADEMPIMENTI

NOTIFICA VIOLAZIONE DATI (art. 33 del GDPR)

In caso di violazione dei dati personali, il Titolare del trattamento notifica alle autorità entro 72 ore dal momento in cui ne è venuto a conoscenza, predisponendo quanto necessario per le notifiche al Garante

PRINCIPALI ADEMPIMENTI

NOTIFICA VIOLAZIONE DATI (art. 33 del GDPR)

In caso di violazione dei dati personali, il Titolare del trattamento notifica alle autorità entro 72 ore dal momento in cui ne è venuto a conoscenza, predisponendo quanto necessario per le notifiche al Garante

PRINCIPALI ADEMPIMENTI

VALUTAZIONE DI IMPATTO PRIVACY (DPIA) (art. 35 del GDPR)

Procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.

E' obbligatoria nei casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il Garante suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.

PRINCIPALI ADEMPIMENTI

VALUTAZIONE DI IMPATTO PRIVACY (DPIA) (art. 35 del GDPR)

Procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.

E' obbligatoria nei casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
La procedura prevede:

1. Condurre l'analisi dei rischi
2. Definire i gap rispetto alla corretta gestione dei rischi
3. Stabilire un Action Plan per colmare questi gap
4. Controllare annualmente gli interventi effettuati per ridurre i rischi

Il Garante suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.

PRINCIPALI ADEMPIMENTI

VERIFICHE GENERALI in sintesi

1) aggiornamento siti Web: aggiornamento dell'informativa privacy del sito web

2) verifica, ed eventuale adeguamento, dei sistemi informatici in uso affinché rispettino i principi di protezione dei dati

3) predisposizione di specifiche autorizzazioni per i soggetti che trattano i dati

4) aggiornamento/formalizzazione dei rapporti contrattuali con eventuali responsabili del trattamento dati (sia interni che esterni)

5)revisione/aggiornamento delle modalità di gestione interna del trattamento dei dati

6) la formazione del personale in materia di privacy