A.G.P.

Associazione Grafologi Professionisti

P R I V A C Y

Regolamento Europeo in materia di protezione dei dati 2016/679

Il 25 maggio 2018 entrerà in vigore, in tutti i Paesi europei, il nuovo Regolamento Europeo in materia di protezione dei dati denominato << GDPR: General Data Protection Regulation>>

Avremo quindi una normativa uguale in tutti i Paese della comunità, in grado di garantire efficacemente e concretamente il diritto alla tutela del dato personale.

Attenzione: di tutti i dati personali, non solo di quelli sensibili.

NON CI SARANNO PROROGHE

Infatti la scadenza è tassativa perché, trattandosi di un Regolamento dell'Unione Europea, è immediatamente efficace senza necessità di recepimento da parte dello Stato italiano.

COSA CAMBIA

Il Regolamento attua una tutela più concreta del dato personale del cittadino attraverso l'introduzione di limiti chiari e precisi sulla modalità di trattamento (cioè di gestione) del dato sia in Italia che all'estero.

Inoltre stravolge il concetto di tutela passando dall'attuale impianto basato su formalismi documentali e di ruoli ad un sistema basato sulla progettazione della tutela (Privacy by design).

CHI È OBBLIGATO A METTERSI IN REGOLA?

Tutti

L'art. 2 del GDPR 679/2016 prevede che il Regolamento si applichi al trattamento dei dati personali (cioè del nome, codice fiscale, email, foto, indirizzo, partita iva, dati bancari, ecc.), in formato cartaceo e/o digitale, contenuti in archivio o destinati a esserci in futuro.

È dunque tenuto al rispetto della nuova normativa Privacy qualunque soggetto, sia persona fisica (professionista, medico, fisioterapista, dentista, ecc.), sia persona giuridica (società di persone o di capitali) che tratti dati personali di terzi per fini non personali e domestici.

Ciò significa che sono tenuti al trattamento dei dati personali in modo corretto e aderente al GDPR tutti coloro che svolgono un'attività economica, di lucro e non (comprese le associazioni).

Il GDPR si applica anche a società, aziende, imprese ed enti con sede legale fuori dall'UE, che trattano però dati personali di residenti nell'Unione Europea.

QUALI AZIONI INTRAPRENDERE?

E' fondamentale effettuare una ricognizione all'interno della propria organizzazione per valutare lo stato dell'arte e valutare le azioni da porre in essere per adeguarsi al nuovo GDPR.

Concretamente, cosa fare?

È necessario verificare chi e come effettua la raccolta dei dati, chi può consultarli e/ o modificarli, come sono conservati, con quali strumenti e con quale diffusione è stata fornita l'informativa ed eventualmente acquisito il consenso al trattamento.

Importante anche analizzare l'organigramma funzionale dei ruoli e degli incarichi.

La mappatura va quindi analizzata alla luce del GDPR e si deve procedere alla redazione di una procedura gestionale che rispetti i nuovi limiti e i nuovi doveri introdotti dal Regolamento.

Questa operazione costituisce la novità essenziale. Solo attraverso l'attività descritta e la successiva progettazione del trattamento sarà possibile dimostrare di aver attuato la sicurezza del trattamento al meglio delle proprie possibilità.

Fondamentalmente, due sono gli aspetti su cui lavorare:

1) aspetti gestionali

verifica dei sistemi rispetto alle misure minime e analisi della sicurezza fisica

2) aspetti documentali

predisporre l'informativa, la lettera di nomina, attuare la formazione e la

sensibilizzazione rispetto alla novità, procedere alla gestione del disciplinare interno

RUOLI

Anche il Regolamento, come già il Codice sulla Privacy, identifica i ruoli dei soggetti attori del

trattamento.

TITOLARE: Persona fisica o giuridica a cui competono tutte le responsabilità nell'ambito di uno specifico trattamento di dati

RESPONSABILE DEL TRATTAMENTO: Figura tecnica qualificata a cui demandare parte delle

responsabilità gestionali.

Le due precedenti figure non subiscono sostanziali modifiche rispetto a quanto già previsto dal D. Lgs

196/2003.

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI = DPO Data Protection Officier

È' la figura professionale identificata dal GDPR a presidio del trattamento dati nei seguenti casi:

- organi o enti o autorità pubblici,
- trattamenti su larga scala (es. supermercati, ipermercati, aeroporti, aziende sanitarie),
- trattamenti su larga scala di dati relativi a reati penali e condanne.

Il DPO deve essere nominato tra figure con elevata qualità professionali e ampia conoscenza specifica.

È una figura obbligatoria nei casi sopra indicati. Ove sia prevista come facoltativa, è consigliabile istituirla.

INCARICATO: Persona fisica che concretamente tratta il dato personale.

CONTITOLARE DEL TRATTAMENTO: E' colui che determina congiuntamente le finalità e i mezzi

del trattamento.

AMMINISTRATORE DI SISTEMA: Sono i soggetti che svolgono le seguenti attività: amministratore di base di dati, amministratore di rete e di apparati di sicurezza, amministratore di sistema software complessi.

A.G.P.

Associazione Grafologi Professionisti

PRINCIPI CARDINE DEL REGOLAMENTO

La nuova norma non parla più di misure minime di sicurezza. Sopprime infatti l'obbligo di adozione di misure minime di sicurezza (firewall, backup, ecc) ma impone la valutazione del rischio rispetto al quale il titolare deve attuare dei comportamenti tutelanti per il trattamento dei dati.

Principio di acconuntability – art. 24: responsabilizzazione del titolare del trattamento

Principio di privacy by design – art. 25: responsabilità progettuale

Quindi dovrà essere comprovata l'organizzazione per garantire la tutela del dato trattato

Principio del diritto all'oblio: possibilità di vedere cancellati i propri dati dal titolare del trattamento compresi i rimandi sui motori di ricerca

Secondo principio (default) - art. 25: obbligo di limitare, in modo predefinito, il trattamento dei soli dati necessari per eseguire il singolo lavoro

INFORMATIVA E CONSENSO

L'informativa deve essere trasparente, comprensibile e completa. Sarà quindi necessario riscrivere le "vecchie" informative alla luce della nuova normativa.

Il consenso deve essere richiesto per specifiche finalità e non in modo generico.

QUALI I RISCHI PER CHI NON SI ADEGUA?

Queste le sanzioni previste per chi non osserva il Nuovo Regolamento Europeo Privacy:

- Ammonizione scritta in caso di una prima mancata osservanza non intenzionale.
- Accertamenti regolari e periodici sulla protezione dei dati.
- Multa fino a 20 milioni di euro o fino al 4% del volume d'affari globale registrato nell'anno precedente.

Per approfondimenti e per il gestionale gratuito http://www.garanteprivacy.it/regolamentoue