

Regolamento Privacy: una nuova sfida per le pubbliche amministrazioni

Autore: Redazione

In:

C'è chi dice che lavorare nella pubblica amministrazione italiana non sia mai stato così impegnativo. Il processo di riforma della PA, che culmina un ventennio costellato di corposi interventi normativi, impone agli uffici pubblici una necessaria rivoluzione culturale e un doveroso adeguamento.

Vuoi essere informato su tutte le novità che riguardano PA Digitale?
Scopri qui il canale dedicato?

Semplificazione, trasparenza, prevenzione della corruzione, digitalizzazione, nuovo Codice dei contratti: queste alcune delle sfide con le quali gli uffici pubblici stanno facendo i conti.

Sfide importanti alle quali bisogna aggiungerne un'altra di cui si parla ancora poco, ma che incombe come una spada di Damocle su tutti gli uffici pubblici e riguarda molto da vicino il processo di innovazione digitale.

Si tratta del nuovo Regolamento Europeo UE 2016/679 in materia di protezione dei dati personali (noto anche come "GDPR" "General Data Protection Regulation").

Il Regolamento ha ad oggetto la "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati" e disciplina "senza necessità di recepimento" - i trattamenti di dati personali, sia nel settore privato che nel settore pubblico.

Il Regolamento è destinato ad abrogare la Direttiva 95/46 che ha portato l'Italia all'adozione del vigente Codice Privacy (D. Lgs. n. 196/2003), norme adottate in un contesto tecnologico completamente diverso, prima che internet, social media, cloud e servizi in rete cambiassero definitivamente il nostro modo di vivere e lavorare. Le nuove norme, tra le altre cose, mirano proprio ad adeguare il livello di protezione dei nostri dati all'evoluzione degli strumenti che utilizziamo.

Il Regolamento è già in vigore e diventerà definitivamente applicabile in tutto il territorio UE a partire dal 25 maggio 2018. Non manca quindi molto tempo, tenendo conto delle complesse attività di adeguamento che devono essere effettuate da chiunque tratti dati personali.

Numerose le novità con cui prendere confidenza nei prossimi mesi, ecco le principali.

Trasparenza

Gli utenti devono essere informati in modo semplice e chiaro (specialmente nel caso di dati di minori) sulle finalità, modalità e ambito del trattamento. E queste informazioni devono essere date per iscritto, anche per consentire agli interessati di esercitare in modo più semplice i propri diritti.

Tutte le novità in tema di trasparenza in questo volume:

La riforma della trasparenza

Luigi Oliveri, 2016, Maggioli Editore

La riforma della normativa sulla trasparenza, il D.Lgs. 33/2013 riscritto in parte dal D.Lgs. 97/2016, mira ad introdurre in Italia un vero e proprio Freedom of Information Act (FOIA), in analogia a quanto fatto, da anni, nei Paesi del Nord Europa ed...

38,00 € 34,20 € Acquista

su www.maggiolieditore.it

Oblio

Viene rafforzato il diritto all'oblio, la possibilità di richiedere, per motivi legittimi, la cancellazione dei propri dati (si tratta di una norma che avrà un impatto assai rilevante per tutti gli adempimenti relativi agli obblighi di pubblicazione per finalità di trasparenza sui siti istituzionali).

Per saperne di più in tema di Diritto all'oblio si consiglia il seguente volume:

Diritto all'oblio: responsabilità e risarcimento del danno

Andrea Sirotti Gaudenzi, 2017, Maggioli Editore

L'opera è un'analisi del diritto all'oblio e delle relative forme di tutela, responsabilità e risarcimento del danno, un supporto pratico che garantisce all'operatore gli strumenti necessari per l'esercizio di un diritto di non...

25,00 € 22,50 € Acquista

su www.maggiolieditore.it

Privacy by design e Privacy by default

Le amministrazioni, come ogni titolare, sono tenute ad adottare misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati (si pensi, ad esempio, all'erogazione di servizi on line e all'implementazione del

sistema pubblico di identità digitale). Inoltre, va garantito l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

Data breach

Viene introdotto il diritto degli interessati di venire a conoscenza delle violazioni dei propri dati personali ("data breach").

Questo significa che nel caso di incidenti di sicurezza relativi ai sistemi usati dalla PA l'amministrazione dovrà organizzarsi per procedere alla notificazione al Garante Privacy senza ritardo (e, comunque, entro le 72 ore). Inoltre, la comunicazione dovrà essere data a tutti gli interessati, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (ipotesi assai probabile per molti dei dati trattati dalle amministrazioni, basti pensare ad esempio a quelli sanitari).

Valutazione d'impatto e registro dei trattamenti

Le amministrazioni, inoltre, sono obbligate ad una valutazione preliminare di impatto sulla tutela dei dati (c.d. "privacy impact assessment"), con una precisa analisi dei rischi con particolare attenzione ai profili della gravità e probabilità dell'evento.

Inoltre, gli enti sono tenuti all'adozione di un registro delle attività di trattamento con descrizione delle misure di sicurezza; si tratta di un adempimento che si rivelerà particolarmente ostico per la gran parte delle amministrazioni che aveva adottato il DPS (Documento programmatico sulla sicurezza) solo come adempimento formale, non curandosi dell'attuazione ed aggiornamento dello stesso.

Data protection officer

Il Regolamento prevede poi l'obbligo per le pubbliche amministrazioni di nominare un DPO - Data Protection Officer (ovvero il responsabile della protezione dei dati personali)

Si tratta di una figura che deve possedere dei requisiti specifici (ad esempio in termini di esperienza e competenza) e deve occuparsi della corretta applicazione della normativa, curando con particolare attenzione della formazione del personale.

Gli enti devono quindi procedere ad individuare il DPO (che può essere interno o esterno) e a dotarlo delle risorse adeguate.

Adeguamento e sanzioni

La protezione dei dati personali, trattata fin qui da molti enti come mero adempimento (se non come alibi per bloccare i tentativi di trasparenza ed innovazione), acquista quindi nuova centralità anche per le pubbliche amministrazioni, chiamate a definire in pochi mesi un percorso di adeguamento efficace che consenta loro di farsi trovare pronte alla scadenza del 25 maggio 2018, evitando così le sanzioni (inasprite rispetto alla disciplina precedente).

Ma, a ben vedere, l'adeguamento delle PA non serve solo ad evitare sanzioni e responsabilità, ma anche e forse soprattutto a garantire quello che, nella società dell'informazione, è un diritto fondamentale degli individui. Un diritto necessario per rinsaldare l'ormai compromesso rapporto di fiducia tra le amministrazioni e i cittadini ed evitare il definitivo fallimento del processo di digitalizzazione.

Scopri qui la Videoconferenza su:

Nuovo regolamento privacy: quali obblighi per la pubblica amministrazione digitale?

<https://www.diritto.it/regolamento-privacy-una-nuova-sfida-per-le-pubbliche-amministrazioni/>