

# Cosa fare per la privacy: se non sei in regola pagherai fino a 10.000.000€

di Paolo Franzese



Cosa fare per la privacy? Chi è soggetto al GDPR? Quando è entrato in vigore il GDPR in Italia? Cosa bisogna fare per la privacy? Cosa prevede il regolamento del 2016? Cercherò di risponderti con questo mio articolo.

## Cos'è il GDPR

**Il 25 maggio 2018 entra in vigore il GDPR** ed abbiamo 6 mesi di tempo per l'adeguamento.

Si tratta del nuovo regolamento sulla privacy e il trattamento dei dati personali in Europa atto a proteggere e responsabilizzare la privacy dei dati di tutti i cittadini dell'UE ridefinendo il modo in cui le organizzazioni di tutta l'area si avvicinano alla privacy dei dati.

Ciò porterà nuove garanzie per i cittadini in quanto verranno introdotte informative e consenso dati più chiare e dettagliate con limiti alla conservazione degli stessi e introduzione di nuovi criteri per il trasferimento dati con un'attenzione molto particolare ai casi di violazione.

Tale nuova normativa coinvolge chiunque abbia a che fare con la raccolta di dati personali.



Cosa fare per la privacy? Partiamo da quali dati raccogli.

## Cosa si intende per dato personale

In base all'art. 4 *“qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che puo? essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o piu? elementi caratteristici della sua identita? fisica, fisiologica, genetica, psichica, economica, culturale o sociale“.*

Ti interessa l'argomento? Iscriviti alla mia newsletter:

Cosa fare per la privacy? Mettiti in regola così...



## Cosa fare per mettersi in regola

Molto dipende dall'attività che svolgete. Infatti ogni piano per affrontare la protezione dei dati deve essere valutato e personalizzato per le esigenze della vostra azienda.

Se siete una [PMI](#), un libero professionista, un freelancer, avete un sito web... innanzitutto dovete verificare che tipo di dati personali tratti la vostra azienda. È sufficiente che raccogliate nomi, cognomi, numero di telefono, email... attraverso la vostra *landing page* o gestiate una *mailing list* per rendere necessario l'adeguamento al GDPR.

A questo punto sarà opportuno valutare quali siano i rischi riguardo il trattamento dei dati personali ed implementare le misure organizzative e tecniche per limitare tali rischi, come ad esempio antivirus validi e aggiornati.

1. Innanzitutto verificate che tutti i vostri applicativi siano affidabili e acquistati con una **regolare licenza d'uso**.
2. Nel caso di furto di dati sarà necessario farne comunicazione entro 72 ore al Garante della Privacy e agli interessati, documentando ogni violazione e fuga dati "*comprese le circostanze, le sue conseguenze e i provvedimenti adottati per porvi rimedio*" (art. 33).
3. La **nomina del DPO è obbligatoria** (art. 37):
  - a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure
  - b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
  - c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.Si tenga presente che la designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto comunitario. Inoltre, anche ove il regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale **designazione su base volontaria**. Il Gruppo di lavoro "Articolo 29", così come il Garante italiano, incoraggiano un tale approccio "cautelativo".
4. La **nomina di un Dpo** (Responsabile della Protezione dei Dati) non sarà necessaria per le PMI in quanto viene specificato dal Garante che nel caso di "*trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti*".
5. Il nuovo **GDPR** ha introdotto una normativa più chiara in merito al consenso e trattamento dei dati personali che dovranno essere espressi con maggior chiarezza. A tal fine le informative su [cookie](#) e privacy presenti sul sito web dovranno essere **maggiormente dettagliate**, redatte in modo chiaro specificando i diritti degli utenti in base alla nuova normativa e citando gli articoli di legge di riferimento del **GDPR**. Si dovranno specificare gli scopi per i quali verranno utilizzati i dati incluse le modalità per chiederne la rettifica e la cancellazione.
6. Se si utilizzano servizi di terze parti si dovrà rimandare alla pagina di policy di questi.
7. Dovrà, inoltre, essere spiegato su quale base vengono forniti i dati, per quanto tempo e con



quali criteri verranno conservati, informando l'utente la possibilità di ricorrere al Garante o all'autorità giudiziaria in caso di utilizzo improprio degli stessi.

8. Il consenso dovrà essere ottenuto con una vera possibilità di scelta e va separato dai Termini e Condizioni del servizio.

Cosa fare per la privacy? Ecco quali sono le sanzioni.

## Le sanzioni in caso di violazione

Le autorità di controllo sono dotate di ampi poteri per garantire che i principi del **GDPR** siano rispettati e le violazioni comportano l'applicabilità di sanzioni amministrative diversificate in questo modo rispetto alla natura, alla gravità e alle conseguenze della violazione:

- per violazioni degli obblighi del titolare o del responsabile come ad esempio rispetto dei principi di privacy by design e privacy by default, meccanismi di certificazione della protezione dei dati, sicurezza..., come previsto dall'art. 83, paragrafo 4, sarà soggetta all'applicazione di sanzioni amministrative pecuniarie fino ad un massimo di **€ 10.000.000** oppure, per le imprese, fino al 2% del fatturato mondiale totale annuo riferito all'esercizio precedente (se si tratta di un importo superiore ai **10 milioni di euro**).
- per violazioni dei principi fondamentali in merito di data protection, diritti dell'interessato o degli ordini delle Autorità di controllo vi sarà una sanzione pecuniaria fino ad un massimo di **€ 20.000.000** oppure, per le imprese, fino al 4% del fatturato mondiale totale annuo riferito all'esercizio precedente (se si tratta di un importo superiore a **20 milioni di euro**).

Riporto alcuni collegamenti a siti in cui riportano aggiornamenti e notizie sul GDPR:

Garante europeo della protezione dati (GEPD): [https://europa.eu/european-union/about-eu/institutionsbodies/european-data-protection-supervisor\\_it](https://europa.eu/european-union/about-eu/institutionsbodies/european-data-protection-supervisor_it)

Garante privacy: <http://www.garanteprivacy.it/regolamentoue>

---

Da un articolo scritto da Paolo Franzese il 21 Maggio 2018