FISCALFOCUS.it
Direttore Antonio Gigliotti

Fiscal Approfondimento
N. 21 Del 03/04/2018

A cura della Redazione

GDPR: la figura del DPO

Il responsabile della protezione dei dati

Categoria: **Privacy**
Sottocategoria: **Disposizioni generali**

Tavola sinottica

Sintesi

Il **nuovo Regolamento (Ue) 2016/679** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (che abroga la Direttiva 95/46/CE - regolamento generale sulla protezione dei dati) è stato pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio 2016, ma la sua piena attuazione è stata prevista a distanza di due anni, dal **25 maggio 2018**.

Focus

L'art. 37 del GDPR prevede una nuova figura professionale designata per qualità professionali e per la conoscenza specifica della normativa, il **DPO** (Data Protection Officer) o **RPD** (responsabile della protezione dei dati).

Sanzioni

Sanzioni amministrative **fino a 20 milioni di euro**, o in caso di un'impresa, **fino al 4% del fatturato** totale annuo mondiale.

Riferimenti Normativi

- Regolamento (Ue) 2016/679;
- D.Lgs. 196/2003;
- Provvedimenti del Garante della Privacy.

Premessa

Il Codice privacy (il D.Lgs. 196/2003) così come gli altri testi di riferimento in materia di protezione dei dati personali vigenti nei singoli Paesi europei è destinato a essere sostituito dal Regolamento UE 2016/679, che costituisce la nuova disciplina privacy per tutti gli Stati membri dell'Unione europea.

Il citato Regolamento, entrato in vigore il 24 maggio 2016, diventerà applicabile in via diretta, senza che sia necessario alcun atto di recepimento interno, in tutti i Paesi UE a partire **dal 25 maggio 2018**.

Pertanto, sebbene fino a tale data rimanga in vigore il nostro Codice privacy, nell'analizzare il quadro normativo di riferimento in materia di protezione dei dati personali non si può prescindere dal richiamare anche il Regolamento UE 2016/679 e dall'esaminare quali siano gli elementi di novità che caratterizzano la nuova disciplina da applicare dal **25 maggio 2018**.

Entro tale data, mancano poco più di due mesi ormai, tutti dovranno applicare le nuove norme, in tutto il territorio dell'Ue, dai grossi colossi quali Google alle banche, alle farmacie, le **PA, le PMI e le organizzazioni no profit**, tutti coloro i quali, in pratica, maneggiano dati degli utenti, anche quelli più basilari.

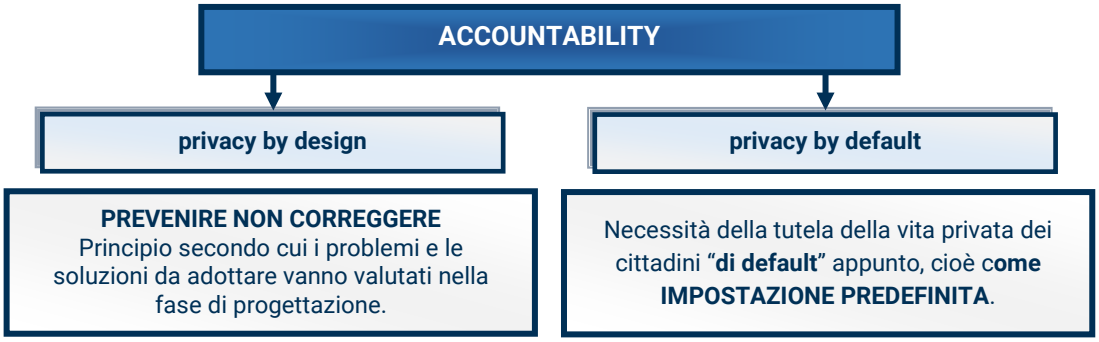
Novità

NOVITÀ

Sostanzialmente **CAMBIA L'APPROCCIO A TUTTO IL SISTEMA**, mentre prima l'obiettivo principale da parte delle aziende era quello di svolgere una serie di adempimenti a cui le stesse dovevano provvedere, ora si pone l'attenzione sul **principio di sensibilizzazione delle imprese**. L'approccio sarà basato, infatti, sul rischio e sulle misure di **accountability** (responsabilizzazione) di titolari e responsabili, ossia, sull'**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento**.

Come adeguarsi alla normativa

Il regolamento generale sulla protezione dei dati (**RGPD**), che esplicherà i propri effetti **a partire dal 25 maggio 2018**, apre le porte ad un profondo cambiamento culturale perché richiede un nuovo approccio all'uso che si fa dei big data, offre inoltre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (**accountability**) con i suoi rami principali la **privacy by design e la privacy by default**.



Come adeguarsi al GDPR in 9 punti

1	**LA VALUTAZIONE DELLA COMPLIANCE**	Raccolta e analisi delle informazioni sull'organizzazione aziendale.
2	CREAZIONE DEL REGISTRO DEI TRATTAMENTI	Un registro delle attività di trattamento svolte sotto la responsabilità del titolare del trattamento.
3	**STESURA/MODIFICA DELLA DOCUMENTAZIONE**	Tutta la documentazione deve essere necessariamente sempre aggiornata e completa.
4	**INDIVIDUAZIONE DEI RUOLI E DELLE RESPONSABILITÀ**	Individuare, sensibilizzare e formare tutte le persone "attive" del processo. Individuare anche le singole responsabilità.
5	**INDIVIDUAZIONE E NOMINA DI UN DATA PROTECTION OFFICER**	Nuova figura professionale - uno degli elementi-chiave del nuovo sistema di governance dei dati - prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici.
6	**DEFINIZIONE DELLE POLITICHE DI SICUREZZA E VALUTAZIONE DEI RISCHI**	Determinazione del valore quantitativo o qualitativo dei rischi connessi ad una situazione concreta o minaccia conosciuta.
7	**VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI**	Consente di valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati.
8	**IMPLEMENTAZIONE DEI PROCESSI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO**	Al fine di assicurarsi di aver adottato tutte le procedure idonee alla tutela dei diritti dell'interessato.
9	**PROCESSO DI DATA BREACH**	Analizzare e fissare gli adempimenti nel caso di un data breach (perdita, violazione ecc…di dati sensibili, protetti o riservati).

Un primo passo da compiere sicuramente sarà la **valutazione della compliance** per poter conoscere tutti i flussi all'interno dell'organizzazione aziendale e valutarne quindi attraverso un'analisi dettagliata tutti i rischi a cui si potrebbe andare incontro definendo pertanto una politica di sicurezza interna. Successivamente altro passo da compiere e da non sottovalutare sarà l'individuazione dei diversi ruoli di tutto il processo e la designazione delle diverse responsabilità.

In tutto ciò i **responsabili della protezione dei dati (RPD)** saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD. Altro adempimento da porre in essere sarà senz'altro l'adozione del **Registro dei trattamenti di dati personali**.

Nota bene

Il DPO va, infatti, considerato come un manager del cambiamento digitale (che è il presupposto su cui è fondato l'intero GDPR) **che deve acquisire conoscenze multidisciplinari per poter garantire in piena autonomia l'assistenza necessaria ai Titolari e/o Responsabili del trattamento nella costruzione di adeguati modelli organizzativi che siano, a loro volta, animati dai principi fondamentali della privacy by default e della privacy by design, nell'ambito dell'accountability**.

Tel. 0968.425805 - E-mail: info@fiscal-focus.it - www.fiscal-focus.it -

La figura del DPO

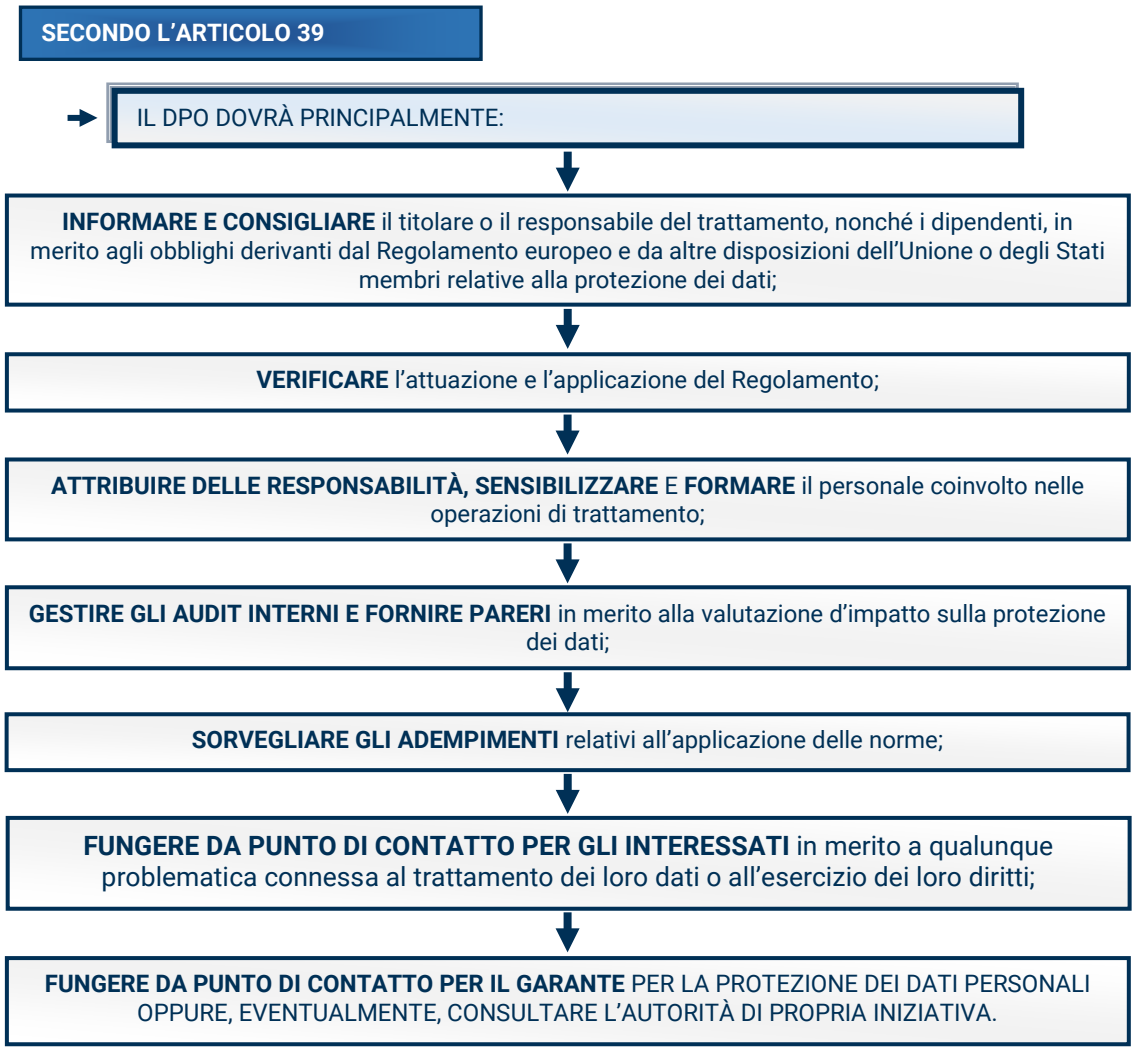
Con l'avvento del nuovo Regolamento (Ue) 2016/679 e per rendere la protezione dei dati ancora più sicura ed effettiva si profila una new entry nel mondo lavorativo, quella del **DPO (Data Protection Officer)** ovvero il Responsabile della sicurezza dei dati (**RPD)**.

Si tratta di una figura di garanzia professionale introdotta dal Regolamento (all'art. 37) designata in funzione delle qualità professionali con conoscenza specifica della normativa e in materia di protezione dei dati il DPO, è il fulcro del processo di "responsabilizzazione" o (**accountability**).

È una figura che ha il diretto coinvolgimento in tutte le questioni e le fasi che riguardano la protezione dei dati personali.

La **responsabilità principale del DPO** sarà quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

Il Regolamento riconosce in tale figura uno degli elementi-chiave del nuovo sistema di governance dei dati e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici.



CHI PUÒ RICOPRIRE IL RUOLO DEL DPO

Il DPO può essere un soggetto esterno oppure direttamente un dipendente del titolare o del responsabile adeguatamente formato e sensibilizzato all'applicazione delle nuove norme.

La scelta del soggetto, infatti, deve avvenire sulla base delle sue indubbie qualità professionali, in particolare in base alla sua conoscenza specialistica della normativa e della prassi e della capacità di assolvere adeguatamente i compiti espressi nell'elenco suddetto (art. 39 del Regolamento), non solo dovrà avere competenze informatiche, di risk management e di analisi dei processi.

Il **DPO è tenuto inoltre al segreto o alla riservatezza** in merito all'adempimento dei propri compiti e può svolgere poi altri compiti e funzioni. Il titolare o il responsabile del trattamento dovranno però assicurarsi che tali compiti e funzioni non diano adito a un conflitto di interessi.

In caso di controversie, lo ricordiamo, sarà proprio il titolare del trattamento a dover dimostrare di aver adottato tutte le precauzioni previste per ridurre al minimo i rischi.

SANZIONI

Tutte le imprese dalle più piccole alle più grandi, chiunque abbia a che fare cioè con l'utilizzo di dati personali, dovranno adottare un sistema di trattamento dei dati fin dall'origine, cioè fin dalla loro acquisizione, su vari livelli, dalla governance, ai processi di comunicazione fino alla cancellazione in banca dati.

L'intero sistema non è da prendere sottogamba, dal momento che la non applicazione comporterà pesanti conseguenze.

Alcune violazioni del regolamento, e i casi più gravi, infatti, sono punibili con **sanzioni pecuniarie fino al 4% del fatturato totale annuo dell'azienda o fino ad un massimo di 20 milioni di euro**.

Attenzione

Mentre **le sanzioni penali rimangono di competenza di ogni singolo Stato**, le nuove sanzioni amministrative, i mezzi di ricorso e le responsabilità che ne derivano sono disciplinate dal nuovo Regolamento, in particolare dal CAPO VIII (Mezzi di ricorso, responsabilità e sanzioni) dall'articolo 77 all'articolo 84.

Ultimi chiarimenti del Garante

Nuovi chiarimenti in arrivo riguardo la nuova figura del DPO (**Data Protection Officer**) o Responsabile della Protezione dei Dati Personali (RPD). Il Garante della Privacy ha pubblicato infatti, il 26 marzo, sul proprio sito istituzionale una scheda informativa per fornire le risposte alle domande più frequenti che sono state sollevate in riguardo al ruolo del DPO nel settore privato.

Requisiti e attestazioni

Il Garante chiarisce inoltre che non sono in realtà richieste specifiche attestazioni formali o l'iscrizione in appositi albi, ma ciò che non deve mancare è certamente la conoscenza approfondita della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Il soggetto idoneo a ricoprire tale ruolo dovrà essere dotato di indubbie capacità professionali, dovrà assicurare la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando l'art. 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.

Quando la designazione è obbligatoria

Altri nodi sono stati sciolti in riguardo all'obbligatorietà della designazione di tale figura all'interno della struttura organizzativa. Il Garante ha fornito importanti chiarimenti anche in merito ai **soggetti che saranno tenuti a nominare il responsabile della protezione dei dati personali**. In particolare, il responsabile della protezione dei dati personali dovrà essere nominato nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Nello specifico, si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "*core business*") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala").

Elenco tracciato dal garante a titolo esemplificativo dei soggetti obbligati

istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; CAF e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

Quando non è obbligatoria

Il Garante ha anche ribadito che nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la **designazione del Data Protection Officer non sarà obbligatoria**. Quindi, ad esempio: in relazione a 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 (vedi art. 97 del Regolamento, in relazione alla definizione di attività "accessoria").

Nota bene

Nonostante la **non obbligatorietà** il Garante ne consiglia e ne raccomanda anche a tali soggetti, in ogni caso, la designazione anche alla luce del principio di **"accountability"** (secondo il principio di responsabilizzazione).

Figura interna o esterna

Il ruolo di responsabile della protezione dei dati personali potrà essere rivestito tanto da un **dipendente** del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti, quanto da un **soggetto esterno**. Potrà essere compatibile con altri incarichi a patto che non vi sia conflitto d'interessi con gli stessi. Proprio per questo, il Garante ha chiarito che sarebbe preferibile non assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT, ecc.).

Nota bene

Nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, da individuarsi comunque in una persona fisica, potrà essere supportato anche da un apposito ufficio dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti.

Qualora il responsabile della protezione dei dati personali sia individuato in un soggetto esterno, quest'ultimo **potrà essere anche una persona giuridica**.

UNICO DPO IN UN GRUPPO IMPRENDITORIALE

Altri chiarimenti hanno precisato circa la possibilità di nominare un unico responsabile della protezione dei dati personali nel caso di un **gruppo imprenditoriale**, a condizione però che tale responsabile sia facilmente raggiungibile da ciascuno stabilimento, e che sia in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

Atto scritto di designazione

Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

Infine, successivamente alla nomina da parte del titolare, come adempimento assolutamente necessario vi è la comunicazione all'Autorità di controllo del nominativo del responsabile della protezione dei dati e i relativi dati di contatto.