# GDPR: conformità e protezione dei dati delle aziende

**INDICE –** GDPR: conformità e protezione dei dati delle aziende PARTE 2



## Portabilità dei dati e responsabilizzazione dei titolari del trattamento

Il Regolamento Generale sulla Protezione dei Dati (GDPR) ha introdotto importanti innovazioni nel contesto della portabilità dei dati e della **responsabilizzazione dei titolari del trattamento**. La portabilità dei dati consente agli interessati di richiedere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivi automatici, al fine di trasferirli da un titolare del trattamento a un altro.

Tuttavia, questo diritto non si applica a trattamenti necessari per compiti di interesse pubblico o legati all'esercizio di pubblici poteri. Allo stesso tempo, **il principio di responsabilizzazione** richiede ai titolari del

trattamento di adottare misure proattive per dimostrare l'applicazione concreta del GDPR e considerare attentamente i rischi che i trattamenti dei dati possono comportare per i diritti e le libertà degli interessati. L'implementazione di misure tecniche, organizzative e di sicurezza adeguate è essenziale per mitigare tali rischi. Queste **novità del GDPR** rappresentano un importante passo avanti nella **protezione dei dati personali** e richiedono la piena conformità da parte dei titolari del trattamento al fine di evitare sanzioni e garantire la sicurezza e la privacy dei dati.

# Data Breach GDPR: linee guida e notifica delle violazioni dei dati personali

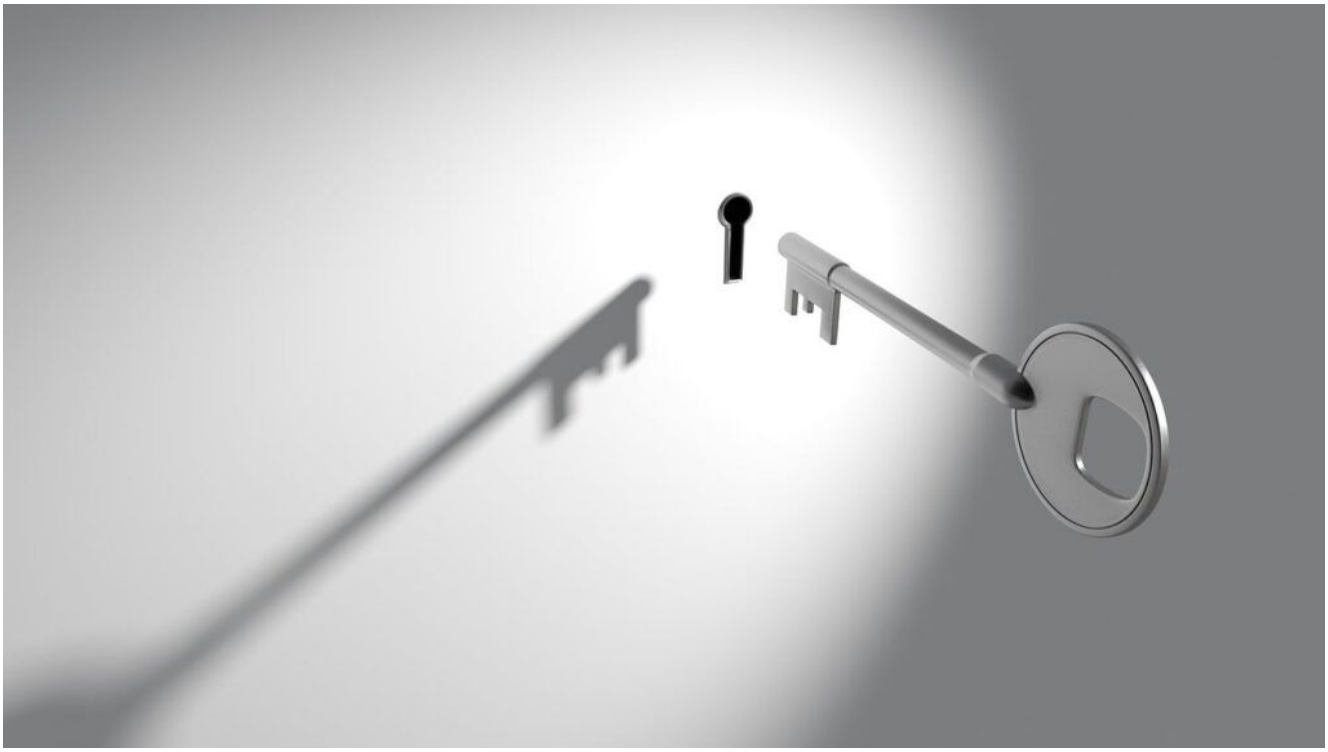
La **gestione efficace di un data breach** nel contesto del GDPR richiede un approccio integrato e una cooperazione a livello europeo. Il titolare del trattamento è tenuto a comunicare al

Garante eventuali violazioni dei dati personali che comportino impatti sui diritti e le libertà degli interessati. Per supportare le organizzazioni in questa gestione, l'EDPB (European Data Protection Board) ha pubblicato le Linee Guida 01/2021 sugli Esempi relativi alla Notifica delle Violazioni dei Dati. Tali linee guida forniscono esempi pratici di data breach e integrano le Linee Guida precedenti adottate dall'ex WP29 (ora EDPB).

Il Garante Privacy nazionale ha anche predisposto un servizio telematico dedicato al data breach, che include un tool di autovalutazione per la notifica delle violazioni dei dati personali. Affrontare adeguatamente un data breach nel rispetto del GDPR è fondamentale per garantire la conformità e la sicurezza dei dati personali.

## Adempimenti e procedure per le imprese secondo il GDPR

L'adozione del **Registro delle attività di trattamento** rappresenta il primo obbligo per le imprese italiane, in particolare per quelle con **almeno 250 dipendenti**. Questo strumento diventa obbligatorio, anche per le imprese con meno di 250 dipendenti, se il trattamento dei dati personali comporta **rischi per i diritti e le libertà degli interessati**, nonché nel caso in cui coinvolga dati sensibili o dati relativi a condanne penali e reati. Il Registro dei trattamenti assume un ruolo fondamentale poiché fornisce un quadro completo delle operazioni di trattamento all'interno di un'azienda o di un ente pubblico, ed è essenziale per valutazioni e analisi dei rischi. Il registro deve essere redatto in forma scritta, compresa la versione elettronica.



Il Registro dei trattamenti contiene le informazioni principali richieste dall'articolo 30 del GDPR, relative alle attività di trattamento svolte dal Titolare del trattamento e, se designato, dal Responsabile del trattamento. Al fine di fornire chiarezza su questo obbligo, il Garante Privacy ha pubblicato FAQ contenenti le informazioni da includere sia nel Registro del Titolare che in quello del Responsabile, nonché le modalità per la sua conservazione e aggiornamento. La corretta adozione e manutenzione del Registro delle attività di trattamento è essenziale per garantire la conformità al GDPR e per rispondere alle richieste del Garante Privacy. Seguire le linee guida e conservare il registro in modo accurato è cruciale per garantire la trasparenza e la protezione dei dati personali all'interno delle organizzazioni.

# Sanzioni GDPR: responsabilità e impatto per le aziende

Le **sanzioni** previste dal GDPR **possono variare da una semplice diffida amministrativa a multe fino a 20 milioni di euro**. È importante comprendere le diverse fattispecie e conoscere le implicazioni delle sanzioni imposte dal GDPR. Oltre alle sanzioni amministrative previste dal regolamento europeo, sono state introdotte anche disposizioni di illeciti penali a livello nazionale.

Per garantire il rispetto delle normative sulla protezione dei dati personali all'interno delle imprese e degli enti, è stata istituita la figura del **Responsabile della protezione dei dati (Data Protection Officer o DPO)**. Il DPO ha il compito di vigilare sull'adempimento delle disposizioni relative alla protezione dei dati personali, utilizzando la propria competenza e conoscenza specialistica della normativa e delle

pratiche in materia.

### Il Responsabile della protezione dei dati:

1. riferisce direttamente alla massima autorità dell'organizzazione;
2. opera in modo indipendente, senza ricevere istruzioni sull'esecuzione dei compiti;
3. riceve risorse umane e finanziarie adeguate a svolgere la propria missione.

Tuttavia, sussistono ancora incertezze riguardo al ruolo del DPO. Sebbene sia una figura rilevante, non è il "fulcro" del sistema delineato dal GDPR, in cui il Titolare del trattamento rimane la figura centrale. Il DPO deve possedere competenze specifiche sulla normativa e le pratiche relative ai dati personali, nonché sulle norme e le procedure amministrative del settore. È altrettanto importante che abbia le capacità professionali necessarie per affrontare le complessità del ruolo, soprattutto nei settori sensibili come quello della sanità, dimostrando competenze specifiche relative ai tipi di trattamento effettuati dal Titolare. L'autonomia decisionale e l'estraneità del DPO nella determinazione delle finalità e delle modalità di trattamento dei dati sono altrettanto importanti per garantire ai soggetti interessati il controllo sulla circolazione dei propri dati.

## Costi del GDPR per le aziende italiane: stime, consigli e strategie di ottimizzazione

Il Regolamento Generale sulla Protezione dei Dati (GDPR) ha introdotto nuove sfide e impatti finanziari significativi per le aziende italiane che devono conformarsi alle sue

disposizioni. Secondo le stime di Idc, **l'adeguamento al GDPR può comportare costi che si aggirano intorno ai 200 milioni di euro per le aziende italiane**, mentre Confesercenti ha stimato una cifra ancora più elevata, pari a 2 miliardi di euro.

Per adeguarsi al GDPR, le aziende devono intraprendere diverse azioni. Tra queste citiamo: la **revisione delle politiche sulla privacy, l'aggiornamento dei sistemi informatici, la formazione del personale e l'implementazione di misure di sicurezza dei dati**. Tutte queste attività richiedono investimenti significativi, soprattutto per le aziende di grandi dimensioni o che trattano un elevato volume di dati personali.

Per ottimizzare la spesa e ridurre i costi complessivi del GDPR, è consigliabile adottare un approccio strategico. Ecco alcuni consigli pratici.

1. **Valutazione delle esigenze**. Effettuare una valutazione accurata delle esigenze specifiche dell'azienda per identificare gli aspetti critici che richiedono maggiori investimenti. Concentrare le risorse sui settori ad alto rischio e dare priorità alle azioni che hanno un impatto significativo sulla conformità.

2. **Pianificazione e budgeting**. Stabilire un piano dettagliato e realistico per l'implementazione del GDPR, includendo una stima dei costi associati a ciascuna attività. Assegnare un budget adeguato e monitorare attentamente le spese durante tutto il processo di adeguamento.

3. **Formazione e consapevolezza**. Investire nella formazione del personale per garantire una migliore comprensione delle disposizioni del GDPR e delle migliori pratiche in materia di protezione dei dati. Un personale ben addestrato può contribuire a ridurre i rischi di violazione e a ottimizzare l'utilizzo delle risorse.

4. **Collaborazione con esperti esterni**. In alcuni casi, può

essere vantaggioso coinvolgere consulenti esterni specializzati in privacy e sicurezza dei dati. Questi professionisti possono fornire competenze specifiche e aiutare a identificare soluzioni efficienti e conformi al GDPR.

5. **Monitoraggio e revisione continua**. Il GDPR richiede un approccio continuo alla conformità. Monitorare costantemente l'ambiente normativo e le migliori pratiche, adattando le politiche e le procedure aziendali di conseguenza. Effettuare regolarmente audit interni per valutare l'efficacia delle misure di sicurezza implementate.

**GDPR: conformità e protezione dei dati delle aziende**

**parte 1**

parte 3

## Hanno parlato di noi

CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

ItaliaOggi

Libero Quotidiano.it

fanpage.it

PANORAMA

TGCOM24

TG5

Rai News 24

Rai 1

Rai 2

Rai 3

Rai Radio 1

CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

ItaliaOggi

Libero Quotidiano.it


# Contattaci

- Orari

Lunedì – Venerdì: 9.00 – 13.00 / 14.30 – 19.00

Lunedì – Venerdì:
9.00 – 13.00 / 14.30 – 19.00

- Email

info@alassistenzalegale.it

- Telefono

+39 3453338510

- WhatsApp

+39 3453338510

Chiamaci
Contattaci

□ Ho letto e accetto i termini dell'Informativa sulla Privacy
Invia