



02_GDPR_Gestire i dati personali



Dato personale

**Qualsiasi informazione
relativa a una persona fisica che,
direttamente o indirettamente,
la identifichi**

Esempi:

- Nome, cognome,
- dati di contatto (email, nr. telefono, indirizzo),
- fattura intestata a un cliente,
- codice identificativo assegnato a un soggetto,
- immagine, fotografia,
- registrazione vocale,
- localizzazione satellitare...



Gestire i dati personali

I dati personali devono essere:

- trattati in modo **lecito, corretto e trasparente**;
- **raccolti per finalità determinate, esplicite e legittime**, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e **limitati a quanto necessario**;
- **esatti** e, se necessario, aggiornati;
- **conservati** in una forma che consenta l'identificazione degli interessati **per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati;
- trattati in maniera da garantirne un'**adequata sicurezza**.

Sono i principi fondamentali denominati:

Liceità, correttezza e trasparenza

Limitazione delle finalità

Minimizzazione dei dati

Esattezza

Limitazione della conservazione

Integrità e riservatezza





- si è responsabili del rispetto delle regole e, in pari tempo,
- è necessario essere in grado di dimostrare la propria conformità.



Accountability, come dimostrarla



1

Raccogli solo i dati realmente necessari

2

Sii trasparente

3

Facilita l'esercizio dei diritti alle persone

4

Decidi i tempi di conservazione corretti

5

Identifica i rischi e proteggi i dati

6

Rendi la conformità un processo costante



1

Raccogli solo i dati realmente necessari

Applica costantemente i principi di liceità, correttezza e trasparenza.

Individua correttamente le finalità e gli obiettivi di ciascun trattamento che esegui, senza “dimenticarne” alcuno e senza pretendere di “fare” attività ulteriori a quelle ufficiali e comunicate.

Non raccogliere dati e informazioni che non sono realmente necessari al perseguimento dell’obiettivo che hai deciso.

Fai in modo che i dati siano sempre esatti e corretti.

Determina il corretto periodo di conservazione, senza “tenere” informazioni che, a ben vedere, non ti servono più.

Adotta, supervisiona e aggiorna le migliori tecniche e misure per proteggere le informazioni che tratti nella tua attività.

Cosa sono le finalità: la finalità è l'obiettivo per il quale raccogli e tratti i dati personali.

Potrebbe essere il reclutamento dei lavoratori, oppure la gestione di un contratto con un cliente.

Rispetta questo obiettivo e non utilizzare i dati per fare altro.





Sii trasparente

Gli individui devono mantenere il controllo dei dati che li riguardano e devono essere **chiaramente informati dell'uso che verrà fatto dei loro dati** non appena verranno raccolti.

In nessun caso i dati possono essere raccolti a loro insaputa e le informazioni devono essere fornite **prima di procedere alla raccolta** dei dati.

Le persone devono anche essere informate dei loro diritti e di come esercitarli.

Non esiste un unico modo per informare adeguatamente le persone ma devi fare in modo di fornire informazioni:

- **adatte alle specifiche situazioni** e ai modi con cui comunichi (è diverso avere clienti con i quali si comunica solo per iscritto via email ed altri che ti contattano solo tramite il sito internet);
- **accessibili e facilmente comprensibili.**



Le icone, per esempio: il Gdpr incoraggia l'utilizzo di soluzioni innovative: puoi mettere in atto un approccio che combina diverse modalità di informazione, in fasi complementari (granulari), a patto di raggiungere l'obiettivo della trasparenza.



Le informazioni sul trattamento dei dati

Quando devo fornirle?

Prima di raccogliervi nel caso di raccolta diretta dei dati: ossia quando i dati sono raccolti direttamente presso le persone (ad esempio con un modulo di acquisto online, la sottoscrizione di un contratto, l'apertura di un conto corrente bancario) o quando sono raccolti tramite dispositivi o tecnologie per l'osservazione dell'attività delle persone (come ad esempio in caso di videosorveglianza, di analisi della navigazione internet, della geolocalizzazione o dell'analisi o del tracciamento wi-fi per la misurazione dell'audience, ecc.).

Entro un termine ragionevole e in ogni caso entro 30 giorni **in caso di raccolta indiretta** di dati personali, ossia quando i dati sono raccolti da partner commerciali, intermediari, fonti pubblicamente disponibili o altre persone, .

Cosa devo indicare*?



La mia identità (ragione sociale o nominativo) e i recapiti



Le finalità (a cosa serviranno i dati raccolti)



La base giuridica per il trattamento dei dati (ossia quale motivo mi dà il diritto di trattare i dati)



La natura obbligatoria o facoltativa della raccolta dei dati e le conseguenze in caso di mancato conferimento dei dati



I destinatari o le categorie di destinatari dei dati (che necessitano di accedervi o riceverli in vista delle finalità definite, compresi i subappaltatori);



Il periodo di conservazione dei dati o i criteri per determinarlo;



I diritti degli interessati



I dati di contatto del responsabile della protezione dei dati dell'organizzazione (DPO), se nominato, o di un punto di contatto in materia di protezione dei dati personali



L'indicazione di poter sempre rivolgersi all'Autorità Garante e proporre reclami





3

Facilita l'esercizio dei diritti alle persone

Gli individui devono mantenere il controllo dei dati che li riguardano.

Ciò presuppone che siano chiaramente informati dell'uso che verrà fatto dei loro dati non appena vengono raccolti.

In nessun caso i dati possono essere raccolti a loro insaputa.

Le persone devono anche essere informate dei loro diritti e di come esercitarli.



È necessario predisporre **procedure che consentano alle persone di esercitare i propri diritti** e rispondere nel più breve tempo possibile a tali richieste di consultazione o accesso, rettifica o cancellazione dei dati o anche di opposizione (a meno che il trattamento non sia effettuato per un obbligo legale incombente sul titolare).

L'esercizio dei diritti è agevolato comunicando un indirizzo al quale rivolgersi e monitorando tutte le richieste.



Decidi i tempi di conservazione

I dati personali hanno, generalmente, un ciclo di vita che, esemplificando molto, può essere così riassunto:

Periodo di conservazione negli archivi e nei database attivi

Durante questo periodo i dati sono conservati per raggiungere gli obiettivi del trattamento.

Ad esempio, in un'azienda, i dati dei lavoratori verranno conservati per tutto il periodo di durata del contratto e, successivamente, anche oltre.

Quelli di un candidato non prescelto verranno conservati invece per un periodo molto inferiore (di solito da 6 mesi a 2 anni al massimo e sempre a condizione che non ne venga richiesta la cancellazione).

In pratica i dati sono facilmente accessibili nell'immediato ambiente di lavoro per le funzioni operative preposte a tale trattamento.

Archiviazione intermedia

I dati personali non sono più utilizzati per il raggiungimento dell'obiettivo prefissato, ma vi è comunque un interesse, per esempio amministrativo, che giustifica il loro trattamento (ad es. la gestione di eventuali contenziosi, ecc.) oppure devono essere conservati per rispondere ad un obbligo di legge (ad es. i dati di fatturazione devono essere conservati per dieci anni, anche se l'interessato non è più cliente). Questi dati potranno essere consultati da soggetti specificamente autorizzati.

Archiviazione finale

Per il loro "valore" e interesse, alcune informazioni vengono archiviate in modo definitivo e permanente.

A differenza dell'archiviazione attiva del database, gli ultimi due passaggi non vengono implementati sistematicamente.

La loro necessità dovrà essere valutata per ogni trattamento e, per ciascuna di queste fasi, sarà effettuato uno smistamento tra i dati.

5

Identifica i rischi e proteggi i dati

«Per “**rischio**” si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di **gravità** e **probabilità**» per i diritti e le libertà

(Linee guida del Gruppo di Lavoro Articolo 29 WP248rev.1)

Il GDPR e l'accountability

Il concetto di accountability comporta che, prima ancora di effettuare operazioni che comportino il trattamento di dati personali,

- **tenuto conto** della natura,
- dell'ambito di applicazione, del contesto e
- delle finalità del trattamento dei dati che intende effettuare, **ma anche**
- **dei rischi che tale trattamento può comportare** per i diritti e le libertà fondamentali delle persone fisiche,

il titolare deve:



mettere in atto misure tecniche e organizzative che siano **adeguate** a garantire che il trattamento sia effettuato secondo i principi espressi dal regolamento stesso. Al contempo, ed è un aspetto molto importante,



ed essere in grado di dimostrare concretamente tale sua responsabilizzazione.

I rischi



I rischi, che hanno **probabilità di accadimento e gravità di conseguenze diverse**, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale. In particolare:

- discriminazioni,
- furto o usurpazione d'identità,
- perdite finanziarie,
- pregiudizio alla reputazione,
- perdita di riservatezza dei dati personali protetti da segreto professionale,
- decifratura non autorizzata della pseudonimizzazione,
- qualsiasi altro danno economico o sociale significativo,
- privazione di diritti e di libertà,
- impedimento all'esercizio del controllo sui dati personali.

Ulteriori e più gravi rischi possono derivare se sono trattati:

- dati personali di carattere particolare (gli ex dati sensibili);
- nel caso si effettuino valutazioni di particolari aspetti personali (il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti);
- dati personali di persone vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.



L'analisi del rischio in breve*

Risk Assessment

Rischio

=

effetto dell'incertezza sugli obiettivi

P X G

Probabilità x Gravità (Impatto)

Definizione del contesto

Identificazione del rischio

Analisi del rischio

Ponderazione del rischio



Trattamento del rischio

* Vedere l'apposita pubblicazione



Proteggi i dati con le misure di sicurezza

Puoi e devi, in effetti, adottare misure di vario tipo.

Organizzative, come policies e procedure:

- per il trattamento dei dati
- per l'esercizio dei diritti degli interessati
- per la gestione degli incidenti
- sull'utilizzo e la configurazione delle misure tecniche e tecnologiche
- sugli strumenti IT aziendali
- sulla data retention

Fisiche, come gli schedari chiusi a chiave, le casseforti, i sistemi anti intrusione o la vigilanza, la videosorveglianza.

Tecnologiche. Tra queste ultime sarebbe opportuno provvedere a definire e documentare i seguenti passaggi:

- predisporre un inventario delle risorse aziendali e dei software
- adottare una configurazione sicura delle risorse e gestire l'inventario degli account, controllando gli accessi alle risorse
- gestire le vulnerabilità
- gestire i log di controllo
- proteggere la posta elettronica, i servizi web e difenderti dal malware
- avere procedure di recupero dei dati
- gestire l'infrastruttura di rete e monitorarla
- formazione e sensibilizzare il personale
- gestire i service provider e la sicurezza degli applicativi
- avere procedure di risposta agli incidenti.

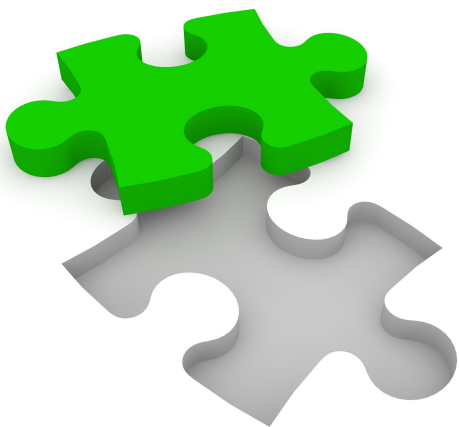
6

Rendi la conformità un processo costante

La conformità non è scolpita nella pietra e fissata una volta per tutte.

Dipende dal rispetto quotidiano, da parte di tutti, a tutti i livelli, dei principi e delle misure previste e attuate.

Controlla regolarmente che il trattamento non sia cambiato, che le procedure e le misure di sicurezza poste in essere siano ben rispettate e, se necessario, adattate e aggiornate.



SL3

_AVV. ANDREA BROGLIA

via della Brunella, 4 - 21100 Varese VA - Italy
Tel +39 0332.811238 - info@studiolegalebrogli.com
www.studiolegalebrogli.com