

00_GDPR_ComeCominciare



CAUTION

Facciamo subito una precisazione

**Il più delle volte
il consenso non serve!**

Ci sono 6 diverse “condizioni” che legittimano il trattamento dei dati.

- 1 Eseguire un contratto
- 2 Adempiere a un obbligo legale
- 3 Tutelare interessi vitali
- 4 Agire nell'interesse pubblico o esercitare di pubblici poteri
- 5 Agire sulla base di un legittimo interesse
- 6 Avere il consenso dell'interessato



In presenza di una delle prime condizioni,
il consenso **non** deve essere richiesto



Creare il Registro delle attività



Gestire i dati personali



I diritti degli interessati



Proteggere i dati



Creare il Registro

Consente di **conoscere i trattamenti che esegui**.

Identificare le principali attività del tuo business che utilizzano dati personali ti fornisce una **panoramica aggiornata e completa dei trattamenti** che devi tenere sotto controllo.

Deve indicare, almeno:

- le **finalità** (ossia l'**obiettivo, lo scopo per il quale raccogli e tratti dati** personali, come ad es.: gestione dei rapporti di lavoro, formazione, gestione dei fornitori, gestione dei rapporti con i clienti, con i prospect, gestione del sito internet, newsletter, campagne promozionali, ecc.);
- le categorie degli **interessati** (dipendenti, clienti, fornitori, ecc.);
- le categorie di **dati personali** (dati comuni, anagrafici, di contatto, dati bancari, ma anche dati “sensibili”, o di geolocalizzazione o di profilazione);
- le categorie di **destinatari** cui trasmetti o comunichi i dati (i fornitori e subfornitori cui demandi attività, come il consulente delle paghe, il consulente del lavoro, il commercialista, la società di informatica che gestisce la sicurezza della tua attività, la società che ti gestisce le campagne pubblicitarie, ecc.);
- i **trasferimenti** verso paesi terzi che eventualmente esegui;
- i **termini di conservazione** dei dati;
- una descrizione generale delle **misure di sicurezza** che adotti per proteggere i dati e le informazioni del tuo business.

Quale Registro utilizzare?



Il Garante della Privacy ha, sul proprio sito, una pagina informativa con molte notizie e consigli utili:

<https://www.garanteprivacy.it/registro-delle-attivit -di-trattamento>.

Alla pagina

<https://www.garanteprivacy.it/home/faq/registro-delle-attivit -di-trattamento> sono disponibili due modelli di registro “semplificati”,

- sia per le attivit  svolte **in qualit  di Titolare** del trattamento, ossia quando decidi autonomamente “perch ” e “come” trattare i dati personali (e solitamente lo fai quando “decidi” di svolgere una determinata attivit  di impresa o d'affari),
- sia **quando**, invece, **assumi la qualifica e il ruolo di Responsabile**, ossia quando esegui dei trattamenti che ti sono demandati da un altro Titolare.





Gestire i dati personali

E' importante, in generale, **ridurre al minimo necessario** la raccolta dei dati, eliminando tutte le informazioni superflue o eccedenti.

E' importante anche **stabilire** con attenzione **chi è in grado di accedere ai (e anche di modificare i) dati** nella tua azienda.

Non dimenticare di **definire con attenzione alcune regole** per la conservazione e, quindi, anche per la cancellazione o l'archiviazione dei dati, che non devono essere conservati più del tempo necessario a perseguire gli obiettivi per i quali sono stati raccolti.

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'adeguata sicurezza.



I diritti degli interessati

Informare le persone

Ogni volta che si raccolgono i dati degli interessati è necessario, prima di farlo, fornire specifiche informazioni sul trattamento e, in particolare, comunicare:

- **perché** stai raccogliendo i dati ("la finalità"; ad esempio per gestire l'acquisto online di un tuo prodotto);
- **cosa ti autorizza** al trattamento di tali dati (la "base giuridica" del trattamento; può trattarsi del consenso dell'interessato, dell'esecuzione di un contratto, dell'adempimento di un obbligo legale, in alcuni casi anche del tuo "legittimo interesse");
- **chi ha accesso ai dati** (i servizi interni competenti, un fornitore di servizi, ecc.);
- **per quanto tempo li conservi** (esempio: "5 anni dopo la fine del rapporto contrattuale");
- le **modalità** secondo le quali gli interessati possono **esercitare i propri diritti** (tramite il proprio spazio personale sul proprio sito web, tramite messaggio ad un indirizzo di posta elettronica dedicato, per posta ad un servizio individuato);
- **se trasferisci** dati al di fuori dell'UE dovrai specificare il paese e il quadro giuridico che assicura il livello di protezione necessario, ecc.).



I diritti degli interessati

Le persone di cui tratti i dati (clienti, dipendenti, fornitori di servizi, ecc.) hanno diversi e importanti diritti sui loro dati:

- innanzi tutto di sapere se tratti i loro dati e, in tal caso,
- il diritto di accesso,
- di rettifica,
- di cancellazione,
- di opposizione a determinati trattamenti,
- di “portabilità” (come per i numeri cellulari),
- di limitazione del trattamento.

Le persone devono poter esercitare efficacemente i loro diritti.

Se hai un sito web, ad esempio, devi fornire un modulo di contatto specifico; è sempre opportuno indicare un numero di telefono o un indirizzo email a cui indirizzare le proprie richieste.

Se i tuoi clienti hanno un account online, devi dare loro la possibilità di esercitare i propri diritti dal proprio account.

- Ricordati di predisporre un processo interno per garantire l'identificazione e l'elaborazione delle richieste in tempi brevi (massimo 1 mese).



Proteggere i dati

A seconda del contesto in cui operi, devi porre in essere **misure che garantiscano un livello adeguato di protezione dei dati che tratti.**

E' importante **analizzare i rischi** che i dati trattati potrebbero comportare per gli interessati, ad esempio se qualcuno non autorizzato vi accedesse, o ne facesse una copia oppure ancora, per esempio, tu non riuscissi più ad accedervi.

I rischi dipendono da molti fattori, come il contesto in cui operi e, ovviamente, il tipo e le categorie di dati che tratti, oltre che dagli obiettivi della tua attività.

A seconda della probabilità e della gravità di determinati eventi, dovrai **valutare quali misure adottare.**

Queste misure possono (e devono) essere **organizzative** (come procedure interne per la gestione del materiale cartaceo o informatico), oppure **fisiche** (come la predisposizione di un antifurto o di una cassaforte per conservare i dati più “sensibili” ma anche e soprattutto **tecnologiche**.

Anche se nel mondo della tecnologia il “rischio zero” non esiste, dovrai proteggere le tue risorse riducendo il più possibile il rischio di perdita, di distruzione, anche accidentale, o di accessi non autorizzati.



Qualche esempio

Proteggere i dati e le informazioni che tratti nel tuo business significa anche tenere costantemente aggiornato l'antivirus e i software che utilizzi, scegliere bene e conservare in modo sicuro le password, adottare, se necessario, la crittografia dei dati, eseguire periodici backup.

Per esempio:

- gli account utente sono protetti da password di sufficiente complessità?
- l'accesso ai locali è sicuro?
- vengono creati profili separati in base alle esigenze degli utenti per accedere ai dati?
- hai una procedura di backup e ripristino dei dati in atto in caso di incidente?

Le violazioni di sicurezza

Gli “incidenti” possono avere conseguenze anche gravi per coloro che ti hanno affidato i dati personali: è importante, oltre che obbligatorio, esserne consapevoli.

Se subisci una violazione dei dati (dati distrutti, persi, alterati, divulgati accidentalmente o illegalmente, accessi non autorizzati, ecc.) devi segnalarlo al Garante della Privacy entro **72 ore** (se ciò può comportare un rischio per i diritti e le libertà delle persone interessate).

Se questi rischi sono elevati dovrai anche informarle direttamente.



SL3

_AVV. ANDREA BROGLIA

via della Brunella, 4 - 21100 Varese VA - Italy
Tel +39 0332 811238 - info@studiolegalebrogli.com
www.studiolegalebrogli.com