



01_GDPR_II Registro delle attività



Creare il Registro

Il registro è previsto dall'articolo 30 del GDPR.

E' un fondamentale **strumento per dimostrare la conformità** alle norme.

E' un documento di inventario e di analisi che **deve riflettere la realtà dei trattamenti** di dati personali eseguiti e che consente di identificare con precisione:

- gli stakeholder (rappresentanti, subappaltatori, corresponsabili, ecc.) coinvolti nel trattamento dei dati;
- le categorie di dati trattati;
- gli interessati dei quali si raccolgono dati personali;
- a cosa servono questi dati (cosa ne fai);
- chi accede ai dati e a chi vengono comunicati;
- per quanto tempo li conservi;
- come sono protetti.

Permette di documentare il trattamento dei dati ma anche di porsi le domande corrette: ho davvero bisogno di questi dati come parte del mio trattamento? È importante conservare tutti i dati per così tanto tempo? I dati sono sufficientemente protetti?, ecc...

La sua creazione e **aggiornamento** sono quindi un'opportunità anche per identificare e dare priorità ai rischi maggiormente rilevanti.

Il Registro, che ha due "forme" (ossia quello **da redigere quando si decidono finalità e mezzi del trattamento** e quello da mantenere **quando si trattano dati per conto di altri**) è uno "strumento" che deve essere costantemente aggiornato.

E' uno dei primi documenti richiesti in sede di verifica e ispezione.



Alla pagina <https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento> sono disponibili due modelli di registro "semplificati".

Il Registro del “Titolare”



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI [per i contenuti vedi Faq sul registro delle attività di trattamento: <https://www.garanteprivacy.it/regolamentoeregistro>]

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE [inserire la denominazione e i dati di contatto]

RESPONSABILE DELLA PROTEZIONE DEI DATI [inserire la denominazione e i dati di contatto]

TIPOLOGIA DI TRATTAMENTO	FINALITÀ E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI [indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI [indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE



Titolare del trattamento: “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali...”.

E' **chi decide “perché”** (per quale finalità, per quale obiettivo) e **“come”** (in quali modi, con quali tecniche) **trattare dati personali**.

Il Registro del “Responsabile”



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE		
<i>[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/registramentoue/registro]</i>		
RESPONSABILE <i>[inserire la denominazione e i dati di contatto]</i>		
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE <i>[inserire la denominazione e i dati di contatto]</i>		
RESPONSABILE DELLA PROTEZIONE DEI DATI <i>[inserire la denominazione e i dati di contatto]</i>		
CATEGORIA DI TRATTAMENTO	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI <i>[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e la "garante" adottate ai sensi del capo V del RGPD]</i>	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Responsabile del trattamento: “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento”.



E' **chi tratta dati per mandato di altri, ossia del titolare** (ad es.: il consulente del lavoro, responsabile, tratta i dati dei dipendenti dell'imprenditore - titolare; il fornitore in cloud tratta - conserva - i dati dell'impresa nel server dedicato).



Tipologie di trattamento

Non tutti i trattamenti sono uguali. Esistono, infatti, diverse tipologie:

Raccolta dei dati: generalmente rappresenta l'inizio del trattamento. Consiste nell'attività di acquisizione del dato;

Registrazione: memorizzazione dei dati su un qualsiasi supporto;

Organizzazione: classificazione dei dati secondo un metodo prescelto;

Strutturazione: attività di distribuzione dei dati secondo schemi precisi;

Conservazione: mantenere memorizzate le informazioni su un qualsiasi supporto;

Consultazione: lettura dei dati personali. Anche la semplice visualizzazione dei dati è un trattamento che può rientrare nell'operazione di consultazione;

Elaborazione: attività con la quale il dato personale subisce una modifica sostanziale. La modificazione differisce dall'elaborazione in quanto può riguardare anche solo parte minima del dato personale;

Selezione: individuazione di dati personali nell'ambito di gruppi di dati già memorizzati;

Estrazione: attività di estrapolazione di dati da gruppi già memorizzati;

Raffronto: operazione di confronto tra dati;

Utilizzo: attività generica che ricopre qualsiasi tipo di impiego dei dati;

Interconnessione: utilizzo di più banche dati, si riferisce all'impiego di strumenti elettronici;

Blocco: conservazione con sospensione temporanea di ogni altra operazione di trattamento;

Comunicazione (o cessione): comunicare dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata;

Diffusione: dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha diffusione anche quando si pubblica online, ad esempio una fotografia su un social network. In assenza di consenso tale attività deve ritenersi illecita;

Cancellazione: eliminazione di dati tramite l'utilizzo di strumenti elettronici;

Distruzione: attività di eliminazione definitiva dei dati.



Trattamento di dati personali: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali".

Il concetto di trattamento comprende, quindi, **tutte le operazioni che implicano una conoscenza, l'accesso o la disponibilità di dati personali**.



Finalità del trattamento

Gli scopi e gli obiettivi per cui si raccolgono e, quindi, trattano dati personali possono essere i più diversi.

Qui di seguito alcuni esempi:

- Assunzione del personale
- Amministrazione del personale
- Gestione dell'assicurazione sanitaria del personale
- Assicurazione per gli incidenti sul lavoro
- Gestione degli adempimenti L. 81/2008
- Controllo degli accessi
- Prevenzione frodi
- Sicurezza fisica
- Gestione dei contenziosi
- Anagrafiche clienti
- Anagrafiche possibili clienti
- Contabilità
- Gestione della contrattualistica con i clienti e i fornitori
- Gestione e recupero crediti
- Pianificazione delle attività
- Pubbliche relazioni
- Ricerche di mercato
- Customer care
- Marketing e comunicazione commerciale
- Analisi della clientela
- Gestione del sito internet
- Gestione dei rapporti di eCommerce
- Gestione newsletter
- ...



Finalità del Trattamento di dati personali: il motivo per cui si raccolgono dati personali.



Basi giuridiche di liceità del trattamento

Il trattamento di dati personali deve essere “sostenuto” da una corretta “motivazione”, ossia da una “base giuridica” o da **una “condizione” che lo renda lecito**.

Quelle che seguono sono le basi giuridiche che il titolare deve individuare per i propri trattamenti:

- A. l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
- B. il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- C. il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
- D. il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- E. il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- F. il trattamento è necessario per il **perseguimento del legittimo interesse del titolare** del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.



Il consenso

E' una **manifestazione di volontà**, espressa con qualsiasi modalità che sia

- **libera**, ossia non “forzata” o non indotta,
- **specificata**, ossia riferita ad un trattamento o ad una modalità precisamente individuata,
- **informata**, ossia resa a seguito della fornitura, all'interessato stesso, di tutte le informazioni rilevanti ed essenziali per comprendere appieno e senza fraintendimenti quali tipologie e modalità di trattamento si vogliono sottoporre alla manifestazione stessa dell'interessato e
- **inequivocabile**, ossia, ancora una volta, si deve trattare di una manifestazione di volontà specifica, esattamente individuata e provabile come certamente “positiva”.

Perché il consenso sia valido è necessario un **atto positivo, chiaro e documentabile**, con il quale la persona manifesti di accettare il trattamento dei propri dati personali.

Si può trattare:

- del completamento di una casella con una X, accompagnato da una firma,
- di un flag su una casella riportante un Sì,
- di un comportamento inequivocabile che sia documentabile e certo e così via.



Il contratto

Il trattamento è lecito quando è **“necessario”** per l'esecuzione di **un contratto** di cui l'interessato è parte, **o per l'esecuzione di attività precontrattuali** che siano richieste sempre dall'interessato.

Nel rapporto di lavoro, per esempio, il datore deve necessariamente trattare una serie di dati relativi ai propri dipendenti, senza i quali non potrebbe adempiere ai propri obblighi datoriali.



L'adempimento di un obbligo legale

Il trattamento è lecito anche nel caso in cui **la normativa** in vigore **imponga al titolare di eseguire determinate azioni** che comportino il trattamento di dati personali.

Sempre nel rapporto di lavoro, per esempio, alcune comunicazioni di dati personali (che sono “trattamento”) agli enti previdenziali, sono imposte da obblighi di legge.



La salvaguardia di interessi vitali

Il trattamento è lecito se il titolare può dimostrare che era o è indispensabile per poter tutelare l'interesse "vitale" dell'interessato o di un altro soggetto: si tratta di ipotesi veramente particolari, "di vita o di morte" dell'individuo e, di conseguenza, di trattamenti eventualmente necessari a preservare l'incolumità o la salute dell'interessato.



L'esecuzione di un compito di interesse pubblico

Il trattamento è lecito, ad esempio, per il perseguimento di un interesse pubblico come quello della prevenzione dei reati o di illeciti, che si sostanzia nello svolgimento di compiti o nell'esercizio di funzioni di natura pubblica o pubblicistica.



Il legittimo interesse

Il trattamento può essere lecito qualora necessario per il perseguimento di un legittimo interesse del titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà degli interessati.

E' importante sottolineare che, mentre nel caso delle altre "basi giuridiche", allorché esse siano presenti, per ciò solo "giustificano" il trattamento dei dati personali (ferme restando le altre prescrizioni del Gdpr), nel caso del legittimo interesse è necessario, di volta in volta, procedere al "**bilanciamento**" degli **interessi** in gioco: quello del titolare e quello dell'interessato.

Qualora l'esito del "test", che è rimesso al titolare e che deve essere documentato, dimostri che gli interessi e i diritti dell'interessato non sono prevalenti sul legittimo interesse del titolare, il trattamento potrà essere effettuato.



Categorie di interessati

Le categorie di interessati sono tutti gli individui dei quali il titolare, l'impresa, può trattare dati personali; o meglio, nell'ottica della predisposizione del registro: dei quali tratta dati personali.

Ad esempio:

- Candidati,
- Dipendenti,
- Clienti,
- Possibili clienti,
- Fornitori,
- Pazienti,
- Cittadini,
- Utenti del sito internet,
- Professionisti,
- Associati,
- Appartenenti alla organizzazione,
- Amministratori,
- Organi di controllo,
- Soci,
- ecc..



Categorie di dati personali

Le categorie di dati possono comprendere:

- Dati personali di tipo comune,
- Categorie particolari di dati personali (ex “sensibili”)
- Dati di identificazione, di contatto, anagrafici e di residenza,
- Dati bancari, finanziari, fiscali
- Dati previdenziali e assicurativi
- Recapiti telefonici, Indirizzo e-mail, Codice fiscale, titolo di studio, cittadinanza, iscrizione al sindacato, dati bancari, stato civile, n° di figli a carico, dati relativi a detrazioni e bonus fiscali, storico lavorativo, fototessera, attestati di formazione, permessi (anche L. 104).
- Rimborsi spese, cessioni e pignoramenti stipendi.
- Dati anagrafici relativi a familiari e affini a carico, o comunque componenti del nucleo familiare, per i quali il lavoratore fruisce di detrazioni fiscali e/o assegni familiari, e/o altri trattamenti economici o normativi così come definito dalla normativa vigente, c. vitae.
- Dati contrattuali.
- Qualifiche ed esperienze professionali
- Immagini, fotografie, filmati, registrazioni sonore in occasione di eventi.
- Dati di navigazione, utilizzo dei servizi informatici.
- Dati di geolocalizzazione,
- Dati genetici,
- Dati biometrici,
- Dati relativi alla salute, alle preferenze politiche, religiose, sessuali,
- Dati di carattere giudiziario relativi a condanne penali e reati,
- Dati relativi a procedimenti giudiziari,
- Ecc..



Categorie di destinatari

Le informazioni da inserire nella relativa scheda o casella possono, secondo il Garante, anche essere indicate semplicemente per categoria di appartenenza, come per esempio gli istituti previdenziali cui si debbano trasmettere i dati dei dipendenti per adempiere agli obblighi contributivi.

In generale si indicano le seguenti categorie:

- Enti previdenziali,
- Fornitori Responsabili o subResponsabili relativamente a determinate operazioni di trattamento che vengano esternalizzate,
- Consulenti e professionisti esterni (Cons. del lavoro, Commercialista),
- Amministrazioni pubbliche,
- Imprese private cui sono demandate attività,
- Banche,
- Assicurazioni,
- Società di gestione dei servizi di comunicazione, marketing, pubblicità,
- Società di gestione dei servizi ICT,
- Fornitori di servizi amministrativi e contabili,
- Fornitori di software, servizi e applicativi in cloud,
- Ecc..



Trasferimenti di dati verso paesi extra UE

Il trasferimento dei dati verso Paesi non appartenenti allo Spazio economico europeo è un aspetto che, in relazione alle odierne modalità di lavoro di tutte le imprese, deve essere attentamente soppesato. Molti servizi e applicativi, infatti, sono ad esempio “made in USA”.

Il concetto di base è quello per il quale la legislazione europea tutela i dati personali e garantisce agli interessati il potere di controllare l'uso che ne viene fatto, dando ad essi la facoltà di esercitare una serie di importanti diritti.

Il Gdpr impone che ogni qualvolta i dati siano trasferiti verso paesi che non hanno simili tutele gli interessati siano ugualmente protetti. La normativa europea, infatti, consente il trasferimento solo a determinate condizioni. In assenza di tali condizioni il trasferimento è vietato.

Le condizioni sono sostanzialmente le seguenti.

- **Decisione di “adeguatezza”** della Commissione Europea (paesi che assicurano un adeguato livello di protezione: non significa un livello di protezione identico ma “essenzialmente equivalente” a quello assicurato all'interno dell'Unione Europea).
- In mancanza di tale decisione il trasferimento può essere effettuato solo se il Paese terzo fornisca **“garanzie adeguate”** e l'interessato abbia effettivi diritti e mezzi di ricorso azionabili per intervenire sui propri dati. Possono costituire garanzie adeguate, ad esempio le seguenti:
 - **Clausole contrattuali** (Clausole Contrattuali ad hoc o Standard SCCs). Nel novembre 2021 la Commissione Ue ha adottato un nuovo set di clausole per allineare le SCC ai nuovi requisiti del Gdpr e riflettere l'uso di nuove e più complesse operazioni di trattamento;
 - **Norme vincolanti d'impresa** (Binding Corporate Rules) approvate, per il trasferimento infragruppo dei dati personali.

In assenza di una decisione di adeguatezza o di garanzie adeguate (SCC e BCR) un trasferimento o un insieme dei trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale può comunque avere luogo in presenza di una delle **deroghe previste dal RGPD (art. 49)**. Si tratta di deroghe ed eccezioni molto particolari.



Schrems 2 e i servizi americani: un accenno

La ormai famosa sentenza “**Schrems II**” (Corte di giustizia UE, Causa 311/18) del 16 luglio 2020 ha invalidato il precedente accordo per il trasferimento dei dati personali verso gli USA, denominato Privacy Shield che veniva ordinariamente utilizzato per “giustificare” i trasferimenti di dati verso fornitori americani. La decisione ha, peraltro, contestualmente riconosciuto valida la decisione della Commissione sulle clausole contrattuali tipo.

E' dunque ad oggi **possibile utilizzare le Clausole come strumento di trasferimento** anche se la Corte ha avvertito che ciò dipende dalla presenza di meccanismi che consentono effettivamente di garantire un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE.

E' dunque necessario verificare che il livello di protezione sia equivalente a quello europeo e, se necessario, è **necessario aggiungere alle Clausole le cd. “misure supplementari”**. Se nemmeno con tali misure fosse possibile garantire il livello equivalente, l'esportatore dei dati è tenuto a sospendere il trasferimento e/o a rescindere il contratto con l'importatore.

Il Comitato dei Garanti europei EDPB (European Data Protection Board) oltre alle FAQ sulle conseguenze del provvedimento del luglio 2020, ha emanato le Raccomandazioni 1/2020 al fine di assistere i titolari nella valutazione caso per caso delle circostanze del trasferimento e nel dovere di identificare e attuare effettive misure supplementari per garantire un livello di protezione sostanzialmente equivalente in caso di trasferimento dei dati verso paesi terzi.

Le indicazioni sulle “supplementary measures” contengono utili suggerimenti.

In sostanza è necessario procedere ad un adeguato assessment per valutare la legittimità del trasferimento, un c.d. Transfer Impact Assessment, basato su diversi step.

Il Comitato Europeo raccomanda di operare con la sequenza che segue:

1. **Mappare i trasferimenti**, verificando che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trasferiti e trattati nel paese terzo.
2. **Verificare lo strumento** su cui si basa il trasferimento (ad esempio SCCs).
3. **Valutare la legge o la prassi del paese terzo** che possa incidere sull'efficacia delle garanzie prestate con lo strumento di trasferimento utilizzato, verificando la legislazione rilevante per il trasferimento e lo strumento di trasferimento. Particolare attenzione deve essere posta sulla legislazione o sulle prassi che disciplinano l'accesso ai dati da parte delle autorità pubbliche. E' necessario basarsi su analisi oggettive, non soggettive e documentare tale passaggio con la dovuta diligenza.
4. **Individuare e adottare le misure supplementari necessarie** per portare il livello di protezione dei dati trasferiti ad un livello sostanzialmente equivalente a quello europeo. Questa valutazione è ovviamente necessaria solo se la precedente disamina rivela che la legislazione del paese terzo incide sull'efficacia del trasferimento. E' possibile servirsi di alcune misure supplementari suggerite dall'EDPB nelle **Raccomandazioni 2/2020**.
5. **Adottare alcuni passi formali**.
6. **Rivalutare periodicamente** il livello di protezione e controllare gli sviluppi che possano influire in tale senso.



Termini di conservazione dei dati

I dati devono essere conservati **per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati.

Possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

E' il principio della **"limitazione della conservazione"**.

In alcuni casi è la legge a stabilire il periodo, in molti altri è compito del titolare indicarlo con precisione.

E' dunque necessario porsi domande come queste:

- Fino a quando ho davvero bisogno dei dati per raggiungere l'obiettivo prefissato?
- Ho un obbligo legale di conservare i dati per un certo periodo di tempo?
- Devo conservare alcuni dati per proteggermi da possibili contenziosi? Quali? fino a quando?
- Quali informazioni devono essere archiviate e conservate? Per quanto?
- Quali sono le regole di cancellazione dei dati?



Misure di sicurezza

Il Registro deve contenere o rimandare ad una elencazione, dettagliata e documentabile, di misure di sicurezza.

Queste misure possono essere:

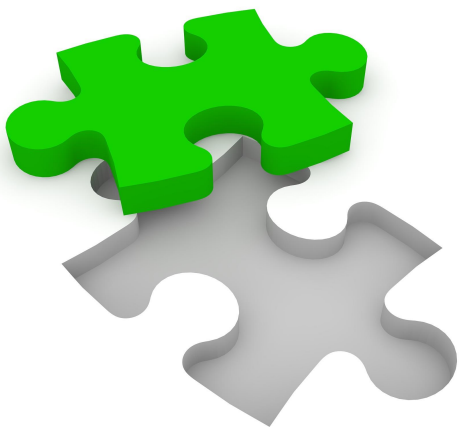
- **organizzative**, come policies e procedure per il personale, ad esempio,
- **fisiche**, come gli schedari chiusi a chiave, le casseforti, i sistemi anti intrusione o la vigilanza, la videosorveglianza,
- **tecnologiche**. Tra queste ultime sarebbe opportuno provvedere a definire e documentare i seguenti passaggi:
 - predisporre un inventario delle risorse aziendali
 - predisporre un inventario dei software
 - adottare una configurazione sicura delle risorse
 - gestire l'inventario degli account
 - controllare gli accessi alle risorse
 - gestire le vulnerabilità
 - gestire i log di controllo
 - proteggere la posta elettronica e i servizi web
 - difendersi dal malware
 - avere procedure di recupero dei dati
 - gestire l'infrastruttura di rete
 - monitorare la rete
 - adottare procedure di formazione del personale
 - sensibilizzare gli utenti
 - gestire i service provider
 - gestire la sicurezza degli applicativi
 - avere procedure di risposta agli incidenti.

Il percorso di adeguamento alle norme inizia dalla consapevolezza dell'importanza degli asset aziendali.

Conoscere e proteggere dati, informazioni, procedure e modalità di business è la via non solo per evitare gravi sanzioni, ma soprattutto per eccellere.

*"I computer sono incredibilmente veloci, accurati e stupidi.
Gli uomini sono incredibilmente lenti, inaccurati e intelligenti.
Insieme sono una potenza che supera l'immaginazione."*

Albert Einstein



SL3

_AVV. ANDREA BROGLIA

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