
# AGEVOLA L'IMPRESA

# SUPPORTA LA BANCA

# GDPR

# Come costruire il Registro di tutte le attività di trattamento Privacy

Come stabilito dall'art. 30 del GDPR, tutti i titolari e i responsabili di trattamento dei dati personali, a eccezione delle imprese e organizzazioni che hanno meno di 250 dipendenti (ma solo se non effettuano trattamenti a rischio), devono tenere un registro di tutte le attività di trattamento dei dati effettuate.

Questo registro è un **documento che dovrà contenere, per legge, una serie di informazioni sulle attività riguardanti il trattamento dei dati personali**, quali:

a. il nome e i dati di contatto del titolare (ed eventualmente del contitolare) del trattamento, del rappresentante del titolare e del responsabile della protezione dei dati;

b. le finalità del trattamento;

c. una descrizione delle categorie di interessati e delle categorie di dati personali trattati;

d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi eventualmente i destinatari di paesi terzi non appartenenti all'Unione Europea od organizzazioni internazionali;

e. nel caso in cui sia previsto, l'indicazione del fatto che i dati personali saranno trasferiti verso un paese terzo o un'organizzazione internazionale, indicando anche di quale paese od organizzazione internazionale si tratta e, inoltre, la documentazione delle garanzie previste;

f. i termini ultimi stabiliti per la cancellazione delle diverse categorie di dati; e infine

g. una descrizione generale delle misure di sicurezza tecniche e organizzative individuate al fine di garantire un livello di sicurezza dei dati personali adeguato al rischio cui gli stessi sono esposti.

Si tratta ovviamente dei contenuti minimi che devono essere indicati all'interno del registro. Dal momento, però, che questo documento non dev'essere visto come un mero adempimento formale, anzi, deve essere inteso come uno strumento operativo, nulla vieta di integrare tali contenuti con qualunque informazione utile al titolare per poter correttamente governare gli aspetti privacy dei trattamenti.

Per redigere un registro dei trattamenti, pertanto, sarà opportuno creare un template in forma tabellare dove, per ogni trattamento, andranno inserite tutte le informazioni richieste.

Il registro dei trattamenti è uno **strumento fondamentale per mappare i flussi di dati all'interno dell'organizzazione**. Infatti, potremmo aggiungere al nostro registro una colonna in cui indicare quali database contengono le informazioni trattate, quali software le processano, quali server sono coinvolti in tali trattamenti, arrivando persino a indicare quali profili sono autorizzati al loro trattamento.

Ancora, potremmo aggiungere l'indicazione sulla necessità o meno, per un determinato trattamento, di essere sottoposto a una **Valutazione d'impatto sulla protezione dei dati**, se questa è stata fatta e se è prevista una nuova valutazione.

Oppure, se il trattamento richiede un consenso, se l'informativa viene correttamente consegnata, o qualunque altra informazione si possa ritenere utile.

È importante capire sin da subito, però, che **il registro dei trattamenti non è un documento che una volta redatto può rimanere fermo e immutabile per sempr**e, dev'essere inteso come un vero e proprio **strumento di lavoro**, e come tale deve essere modificato e deve essere mantenuto aggiornato, e sempre attuale.

Per raggiungere questo scopo è fondamentale innanzitutto individuare, all'interno dell'organizzazione, **i soggetti che hanno la più ampia visione delle attività di trattamento e coinvolgerli nella redazione e aggiornamento del registro dei trattamenti**, responsabilizzandoli sull'importanza di tale attività. È necessario renderli edotti dei vantaggi e del valore aggiunto che una gestione trasparente dei flussi di dati personali rappresenta per l'azienda.

Per quanto concerne i **soggetti obbligati** alla tenuta del registro dei trattamenti, come risulta dall'art. 30, paragrafi 2 e 3 essi sono tanto il **titolare quanto il responsabile del trattamento** o, se presenti, i loro **rappresentanti.**

Su entrambi incombe pertanto uno specifico dovere in tal senso, tenendo però conto che, dal punto di vista del contenuto, nel caso in cui il registro sia tenuto direttamente dal titolare del trattamento, o dal suo rappresentante, avrà una portata più estesa, invece qualora esso sia tenuto dal responsabile del trattamento, o dal suo rappresentante, dovrà indicare obbligatoriamente (ma ogni ulteriore informazione sarà sempre utile, nell'ottica del GDPR) solo:

- i contatti del titolare, del responsabile del trattamento e dei loro rappresentanti, se presenti, nonché del responsabile della protezione dei dati;
- le categorie di trattamenti effettuati per ciascun titolare del trattamento;
- il trasferimento dei dati ad un paese terzo (extra-europeo) o ad un'organizzazione internazionale, specificando di quale paese o organizzazione si tratta ed evidenziando le adeguate garanzie previste per il trasferimento stesso; e infine
- se possibile, la descrizione delle misure di sicurezza tecniche ed organizzative adeguate ai rischi preventivati.

Il registro delle attività di trattamento si configura come uno strumento fondamentale non soltanto ai fini di eventuali controlli di legittimità da parte del Garante, ma anche perché consente di avere a disposizione un quadro aggiornato dei trattamenti che vengono realizzati nell'azienda, organizzazione o soggetto pubblico. Quest'ultima circostanza sarà importante, in particolare, per poter realizzare una corretta ed efficace analisi e valutazione dei rischi.

Da un punto di vista strettamente formale, il GDPR non detta delle regole generali né individua le concrete modalità attraverso cui il registro delle attività di trattamento dovrà essere formato.

L'art. 30 si limita infatti a precisare che il registro delle attività di trattamento dei dati dovrà essere tenuto in forma scritta, su supporto tangibile oppure, e preferibilmente, in formato elettronico, e dovrà inoltre essere messo a disposizione su richiesta dell'autorità di controllo (nel caso dell'Italia, il Garante per la protezione dei dati personali).

Al contrario poi di altri adempimenti sanciti dal nuovo Regolamento europeo a titolo obbligatorio, la predisposizione di un tale registro delle attività di trattamento **non è un adempimento formale**. Esso si configura, piuttosto, come uno strumento che è parte integrante di quel generale sistema di corretta gestione dei dati personali che le aziende, organizzazioni o soggetti pubblici dovranno creare.

Un'adeguata predisposizione del registro delle attività di trattamento potrà essere, infatti, un elemento importante al fine di realizzare un corretto trattamento dei dati personali, in linea quindi con l'obiettivo di responsabilizzazione (la c.d. accountability), che, come precisato in più occasioni in questo Speciale di approfondimento sul GDPR, è uno dei principi fondamentali che il legislatore europeo ha voluto incentivare maggiormente e su cui fonda l'intera disciplina del Regolamento.

La necessità di dimostrare la legittimità del trattamento dei dati, e di conseguenza la sua conformità alla disciplina dettata dal GDPR, prescinde dalle dimensioni effettive dell'organizzazione aziendale, e quindi in un panorama di questo tipo il registro diventa un valido strumento per tutte le organizzazioni.

Proprio per questa ragione, su indicazione del Garante della Privacy, tutti i titolari ed i responsabili del trattamento dei dati, a prescindere dalle dimensioni dell'organizzazione (e quindi anche qualora vi siano meno di 250 dipendenti), sono invitati a predisporre un tale registro.

In ogni caso, anche se tale registro non verrà predisposto, è necessario che i titolari e i responsabili del trattamento si impegnino per effettuare in altro modo una scrupolosa individuazione dei trattamenti posti in essere e delle loro caratteristiche principali.

D'altra parte, come visto più sopra, i contenuti del registro dei trattamenti, delineati dall'art. 30, possono essere integrati anche con altre informazioni da parte del titolare o del responsabile, i quali potranno infatti inserire ogni elemento aggiuntivo, se lo riterranno opportuno alla luce della complessiva valutazione d'impatto sulla protezione dei dati e sulla base delle attività di trattamento svolte.

Il registro dei trattamenti, quindi, è uno strumento fondamentale non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, ma è anche **indispensabile per ogni valutazione e analisi del rischio** (ulteriori adempimenti previsti dal GDPR in ottica accountability).

Il Garante per la protezione dei dati personali, nella sua **Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali ritiene che: "il registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali"**, invitando tutti i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro.

**Il Garante si rivolge, quindi, a tutti i soggetti, prescindendo dalle dimensioni dell'organizzazione.**

Il registro dei trattamenti dovrebbe essere gestito in maniera centralizzata, garantendo l'accesso a tutte le persone coinvolte nel suo mantenimento onde evitare la proliferazione di copie che renderebbero difficile identificare la versione più aggiornata.

Le sanzioni amministrative pecuniarie previste dal Regolamento ammonteranno fino a 20 Milioni di Euro o fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente.

Ma coloro i quali decideranno di impegnare risorse ed energie in un tale progetto si troveranno ad avere una mappatura ordinata e organizzata che, da un lato in caso di visita ispettiva da parte del Garante dimostrerà una profonda attenzione alle tematiche di protezione dei dati personali; dall'altro consentirà all'organizzazione di tenere sotto controllo quali tipi di dati sono in fase di trattamento, da chi (quali servizi o unità aziendali) e per quali finalità. Una tale conoscenza consentirà ai titolari di ottimizzare le operazioni di trattamento limitando gli sprechi in termini di tempo, risorse e duplicazione delle informazioni, abbattendo anche i rischi di eventuali trattamenti illeciti o contestazioni.

Via Vandelli, 20  22100  Como

Tel. 031.2077468 | mediazione@novaria.eu

Iscr. OAM n. M0353

Via Q. Sella, 4  28073  Fara Novarese (NO)

Tel. 800.926266 | agevolato@novaria.eu

Via Vittorio Emanuele III, 353  90049  Terrasini (PA)

Tel. 091.8684675

RICHIEDI ANALISI GRATUITA

**Novaria**