LA TENUTA DEI REGISTRI: CONSAPEVOLEZZA, *ACCOUNTABILITY*, *SUBSTANCE OVER FORM* E DOCUMENTAZIONE DELLE SCELTE.

IL CONTENUTO E LA FORMA DEI REGISTRI. QUALI ONERI PER TITOLARI E RESPONSABILI?

avv. Giacomo Conti
manager

I REGISTRI DEI TITOLARI E DEI RESPONSABILI: UNO, NESSUNO O CENTOMILA?

Il registro delle attività di trattamento può essere tenuto dal Titolare o dal Responsabile del trattamento (Art. 30 GDPR).

Il registro delle attività è un imprescindibile strumento di accountability e consapevolezza.

CHI HA L'OBBLIGO DI TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO?

L'art. 30 GDPR esenta dall'obbligo di tenuta dei registri le sole imprese o organizzazioni con meno di 250 dipendenti.

Il WP29 (ora EDPB) e l'Autorità Garante Italiana hanno, tuttavia, di fatto esteso quest'obbligo a tutti i titolari e responsabili.

Tutti i titolari e responsabili che effettuano attività di trattamento di dati personali dovrebbero dotarsi di un registro delle attività di trattamento.

Per impostare corrette operazioni di trattamento di dati personali in azienda non basta realizzare il solo registro delle attività di trattamento, ma occorre realizzare altri tipi di registri, pure se il GDPR non li prevede espressamente.

QUALI SONO I REGISTRI CHE DOVREBBERO ESSERE NECESSARI PER REALIZZARE UNA CORRETTA *ACCOUNTABILITY* IN AZIENDA?

A. IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL TITOLARE E DEL RESPONSABILE (ART. 30 GDPR).

B. IL REGISTRO DELLE VIOLAZIONI/*DATA BREACH* (ART. 33 GDPR).

C. IL REGISTRO DELLA FORMAZIONE DEI COLLABORATORI E DEI DIPENDENTI (ART. 29 GDPR).

IL REGISTRO DELLE VIOLAZIONI (ART. 33 GDPR)

Ai sensi dell'art. 33 c. 5 GDPR stabilisce che: "*Il titolare del trattamento* ***documenta qualsiasi violazione*** *dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo*."

Senza una corretta e precisa annotazione della violazione può essere difficile valutare la gravità della violazione subita ed il rischio che questa presenta per gli interessati.

IL REGISTRO DELLA FORMAZIONE DEI COLLABORATORI E DEI DIPENDENTI (ART. 29 GDPR).

L'art. 29 GDPR supera la vecchia nozione formale di incaricato e parla, invece, di soggetti autorizzati ed istruiti ad operare attività di trattamento sotto l'autorità del titolare.

I soggetti autorizzati devono essere formati ed istruiti, anche in ragione delle responsabilità e dei compiti che rivestono in azienda.

Ogni titolare e responsabile ha il dovere di istruire i soggetti che, sotto la sua autorità, effettuano attività di trattamento di dati personali degli interessati.

Sembra, quindi, necessario documentare l'attività formativa erogata a favore dei propri dipendenti.

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO (ART. 30 GDPR)

In che cosa consiste il registro delle attività di trattamento?

Il registro delle attività di trattamento è un importante strumento di consapevolezza e documentazione.

In esso il titolare (o il responsabile) documenta le attività di trattamento che effettua in azienda ed è un importante strumento e si può considerare, pertanto, come una mappatura dei trattamenti effettuati in azienda.

Chi è obbligato alla sua tenuta?

E' un obbligo che ricade sia sui Titolari che sui Responsabili del trattamento.

Il Garante della Protezione dei dati italiano e l'ex WP29 (ora EDPB) hanno, di fatto, esteso quest'obbligo a tutti i titolari e responsabili che effettuano trattamenti di dati personali valorizzando l'importanza strategica di questo documento.

Perché è importante il registro delle attività di trattamento e quale è la sua funzione?

Il registro delle attività di trattamento è uno strumento imprescindibile di consapevolezza.

La tenuta corretta di un registro delle attività di trattamento è alla base dei successivi adempimenti previsti dal GDPR.

Un registro correttamente compilato permette al Titolare di tenere sotto controllo i flussi, i rischi ed i trattamenti che effettua in azienda e, se del caso, di agire proattivamente nell'ottica della prevenzione del rischio.

Esso rappresenta, non da ultimo, un importante strumento di trasparenza e di cooperazione con l'Autorità di controllo.

Quale forma deve (o dovrebbe avere) avere il registro?

Ai sensi dell'art. 30 comma 3: "*I registri di cui ai paragrafi devono essere tenuti in forma scritta, anche in formato elettronico*."

La disposizione normativa solleva importanti problematiche applicative.

Alcuni ritengono che il registro debba avere data certa e debba essere firmato e sottoscritto (anche digitalmente),

Altri ritengono che possa bastare tenerlo in forma libera (ad esempio in formato Excel)

La seconda tesi opera un'estensione analogica del concetto di forma scritta trasformando il dato letterale della norma nel senso di forma documentabile che sembra essere compatibile con lo spirito del GDPR.

Vi sono, in ogni caso, molti gestionali che sono in grado di aiutare titolari e responsabili a tenere i registri.

La prassi in materia, tuttavia, non si è ancora consolidata né il garante ha assunto formale posizione in un senso o nell'altro.

VEDIAMO LE TESI SULLA FORMA DEL REGISTO

TESI A: Il registro deve avere data certa e debba essere firmato e sottoscritto (anche digitalmente),

FORMA SCRITTA = SOTTOSCRIZIONE E DATA CERTA

TESI B: il registro può essere nella forma che il Titolare o il responsabile preferiscono anche, ad esempio, in PDF, Excel o Word.

FORMA SCRITTA = FORMA DOCUMENTABILE.

FOCUS: IL CONTENUTO DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il contenuto minimo del registro è definito dall'art 30 GDPR c.1:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento 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;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il registro, ove tenuto dal responsabile ai sensi dell'art. 30 c. 2 GDPR deve indicare, inoltre:

a. il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

La legge detta, quindi, requisiti di contenuto minimo per il registro delle attività di trattamento.

Come spesso accade in questa materia, tuttavia, non sempre il rispetto dei requisiti di legge può ritenersi bastevole a rendersi *compliant*.

Il registro deve, infatti, essere articolato e sviluppato secondo le concrete esigenze aziendali che devono provvedere ad integrare il registro secondo le proprie concrete esigenze organizzative.

FOCUS: LA FORMA DEL REGISTRO

In ambito giuridico, con il termine 'forma' si indica – in estrema sintesi – sia il modo e/o la figura esteriore con cui l'atto giuridico si presenta, sia il mezzo con cui il contenuto di un atto è immesso nell'intersoggettività giuridica; attraverso la forma, la volontà, da mero fenomeno psichico, si sostanzia in atto giuridico, e – unitamente a quest'ultimo – diviene riconoscibile agli altri consociati. **La forma del negozio è il veicolo della volontà.**

Il termine '*forma*' è dunque essenzialmente riconducibile:

a. all'aspetto manifestativo dell'atto, che mantiene autonoma rilevanza rispetto al cd. 'contenuto sostanziale',

b. ovvero alle modalità attraverso cui l'atto deve essere compiuto per spiegare certi effetti, o al mezzo espressivo mediante il quale l'esistenza, la validità, l'efficacia e/o finanche il contenuto dell'atto devono trovare riscontro.

NEL SILENZIO DEL GARANTE ITALIANO COSA HANNO DETTO LE ALTRE AUTORITÀ STRANIERE?

Molte autorità Garanti di Stati Membri (come il CNIL) hanno proposto facsimili di registro in diverso formato: Excel (Autorità Garante Belga), RFT/Word (Autorità Garante Francese), ma nessuna si è espressa circa il requisito formale del Registro delle attività.

Molte autorità Garanti di Stati Membri (come il CNIL) hanno proposto facsimili di registro in diverso formato: Excel (Autorità Garante Belga), RFT/Word (Autorità Garante Francese), ma nessuna si è espressa circa il requisito formale del Registro delle attività.

Il modello di registra delle attività di trattamento fornito dal CNIL, tuttavia, richiede la sottoscrizione del titolare o del responsabile che è tenuto alla compilazione di questo.

L' ART. 20 COMMA 1*BIS* DEL CAD ED IL CONCETTO DI FORMA ELETTRONICA DEL DOCUMENTO NELL'ORDINAMENTO ITALIANO

"*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile* ***quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata*** *o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.*

In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità*. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida*."

Il GDPR ha, però, portata a livello Europeo e l'interpretazione data dal nostro Codice dell'Amministrazione Digitale potrebbe essere restrittiva.

LA POSIZIONE PRESA DALL'AUTORITÀ GARANTE BELGA

Secondo l'Autorità Garante belga i registri interni devono essere:

1. resi disponibili per iscritto, anche in forma elettronica.

2. chiari e facilmente comprensibili per l'Autorità Garante.

3. creati in formato può essere flessibile al fine di soddisfare le esigenze di ogni tipo di trattamento.

4. da ultimo, i registri interni devono essere costantemente aggiornati.

Per l'Autorità Garante belga, quindi, il concetto di forma documentabile e consultabile sembra non coincidere necessariamente con quanto prevede il nostro CAD.

QUELLE EST LA POSITION PRISE PAR LA CNIL?

"*Le registre de traitement* ***doit recenser l'ensemble des traitements mis en œuvre par votre organisme*****."**

Il registro delle attività di trattamento deve mappare l'insieme dei trattamenti posti in essere dalla vostra organizzazione.

"*La CNIL recommande, dans la mesure du possible, d'enrichir le registre de mentions complémentaires afin d'en faire un outil plus global de pilotage de la conformité*."

Il CNIL raccomanda, per quanto possibile, di arricchire il registro arricchire il registro di ulteriori informazioni al fine di renderlo uno strumento più globale per la gestione della conformità.

CONCLUSIONI

Il registro è uno strumento di consapevolezza e responsabilizzazione che può essere tenuto dal titolare e dal responsabile nella forma che ritiene preferibile purché la stessa sia documentabile e facilmente intelleggibile.

Il registro non deve essere visto come un adempimento burocratico-statico, bensì dinamico e si deve prediligere una forma che ne consenta – se necessario – il periodico aggiornamento.

È possibile anche tenere il registro con dei gestionali studiati allo scopo.

GRAZIE