La privacy impone il Registro dei dati nelle aziende con più di 250 dipendenti

PRIVACY

«Libro» anche per le Pmi sottosoglia con gestione continua di informazioni

Sanzioni fino a 20 milioni o fino al 4% del fatturato per chi non si allinea

Pagina a cura di
Daniele Colombo

Grandi aziende chiamate a redigere il Registro del trattamento dei dati. È uno degli adempimenti più importanti previsti dal Regolamento europeo per la protezione dei dati personali, in vigore dal 25 maggio. Ma in che cosa consiste il Registro e quale è il suo contenuto? Quali sono i soggetti aziendali obbligati a redigerlo e le modalità di aggiornamento?

Il contenuto del Registro
Il Registro è il documento che contiene le attività di trattamento dei dati, redatto preferibilmente in formato elettronico (ad esempio su un foglio excel) per facilitarne l'aggiornamento periodico. L'obbligo di tenuta e di aggiornamento grava sulle organizzazioni medio-grandi, ossia quelle con 250 o più dipendenti (articolo 30 del regolamento 679/2016).

Per le più piccole, il Regolamento Ue prevede un'esenzione limitata, stabilendo che queste debbano documentare i trattamenti solo se:
- sono suscettibili di comportare un rischio per i diritti e le libertà delle persone;
- non sono occasionali;
- coinvolgono categorie di dati particolari o dati relativi a condanne penali o dati giudiziari.

Ci sono, infatti, realtà che, sebbene abbiano meno di 250 dipendenti, trattano dati relativi, ad esempio, a clienti o dati personali relativi alle risorse umane, in maniera non occasionale. In questi casi, la non occasionalità del trattamento impone la tenuta del Registro.

Il «considerando» 75 del Regolamento specifica che i rischi per i diritti e le libertà delle persone fisiche possono derivare da trattamenti di dati personali suscettibili di causare un danno fisico, materiale o immateriale (ad esempio, discriminazioni, furto o usurpazione d'identità). C'è poi un rischio se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza. Ancora, c'è un rischio se sono trattati dati personali di persone fisiche vulnerabili, in particolare di minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Le figure aziendali coinvolte
La responsabilità di redigere, aggiornare e tenere correttamente il Registro è in capo al titolare del trattamento e al responsabile del trattamento.

Nelle aziende più strutturate e suddivise in dipartimenti, sarà possibile anche delegare uno o più soggetti interni che si occupino della registrazione e dell'aggiornamento di trattamenti specifici relativi alla propria area (ad esempio un modulo trattamenti dell'area marketing).

Le informazioni contenute nel singolo modulo di area potrebbero poi confluire nel Registro delle attività di trattamento centralizzato, il cui accesso potrebbe essere consentito solo al Titolare del trattamento e al Responsabile per la protezione dei dati (il Dpo), che, se presente, ha il compito di fornire assistenza nella redazione e di verificare la corretta tenuta dei registri.

Il titolare del trattamento, se la struttura organizzativa è particolarmente complessa, potrebbe anche incaricare con un atto scritto un responsabile della tenuta del Registro delle attività di trattamento. Le informazioni contenute nel registro devono essere periodicamente aggiornate per "fotografare" la situazione aziendale relativamente al trattamento dei dati personali. L'aggiornamento, pertanto, è richiesto ogni qual volta si verifichino rilevanti cambiamenti che incidono sui trattamenti dei dati personali. In altri termini, il Registro non è un documento statico, ma dinamico, da aggiornare tutte le volte che ci sono variazioni o modifiche relativamente al trattamento di dati personali. In caso di mancato rispetto degli obblighi di tenuta e aggiornamento del Registro, laddove obbligatorio, i titolari e i responsabili del trattamento potranno subire sanzioni amministrative molto pesanti, per importi fino a 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo.

PAROLA CHIAVE

Gdpr

Il nuovo Regolamento Ue
«Gdpr» è la sigla che indica il nuovo Regolamento europeo sulla protezione dei dati personali, in inglese «General data protection regulation». È il Regolamento Ue 679 del 2016, in vigore dal 25 maggio, che punta a rafforzare la tutela dei dati personali dei cittadini europei e a rendere omogenea la normativa sulla privacy nella Ue. Dalla sua entrata in vigore, il Gdpr ha abrogato, in Italia, le norme del Codice per la protezione dei dati personali (Dlgs 196/2003), nelle parti con esso incompatibili.

© RIPRODUZIONE RISERVATA

LA BUSSOLA PER IL REGISTRO

1. Chi deve tenere il Registro del trattamento dei dati
Il Registro deve essere tenuto dal titolare del trattamento dei dati e, se sono presenti, dal contitolare del trattamento o dal rappresentante del titolare del trattamento

2. Che cosa deve contenere
Il Registro deve contenere:
- il nome e i dati di contatto del responsabile del trattamento dei dati
- le finalità del trattamento, che varieranno a seconda dalla tipologia di dato, relativi a dipendenti, fornitori e clienti
- le categorie di interessati al trattamento, ad esempio dipendenti, clienti, fornitori
- i destinatari della comunicazione dei dati
- l'eventuale trasferimento dei dati a Paesi terzi
- i termini di cancellazione dei dati
- le misure di sicurezza tecniche e organizzative adottate con l'obiettivo di tutelare i dati

3. La forma
Il Registro del trattamento dati deve essere tenuto in forma scritta, anche in formato elettronico (in un foglio word, o excel)

4. Lo scopo del document
Il registro deve:
- dimostrare che la gestion dei dati è conforme ai princ del Regolamento Ue 679/2
- mettere a disposizione i d necessari alle autorità di controllo

5. A quali reparti aziendali chiedere i dati
Coloro che redigeranno il Registro del trattamento d dati, dovranno fare riferimento per le informazioni necessarie a diversi reparti aziendali:
- reparto commerciale
- reparto vendite
- amministrazione e contro
- ufficio risorse umane
- reparto IT
- reparto sicurezza
- reparto marketing