Confagricoltura
Padova

Adeguarsi al GDPR

I passi da fare

1. Aumentare la consapevolezza

A prescindere dalle dimensioni della vostra azienda, **informatevi e informate il vostro personale dell'arrivo del Gdpr** e della maggior accortezza necessaria nel processare i dati dei clienti, così come nell'impostare adeguate procedure di sicurezza sui computer.

Ad esempio: niente più post-it sullo schermo con la password, non lasciare il computer accessibile quando si va in pausa pranzo, non consentire l'accesso ai dati a tutti i dipendenti dell'azienda se non ve ne è motivo.

2. Verificare le informazioni e i dati che si posseggono

Capire che tipo di dati si trattano nella propria attività, da dove vengono e con chi si condividono, inclusi i servizi e i software che li gestiscono.

Che programma usate per le mail, il cloud o la newsletter? Sono affidabili? Avete una regolare licenza d’acquisto?

3. Individuare ruoli e responsabilità

Nominare un responsabile del trattamento interno o esterno.

→ Nomina responsabile del trattamento Confagricoltura e Unione Agricoltori di Padova

4. Redigere e tenere un registro dei trattamenti

Documento volto a tenere traccia dei trattamenti effettuati da parte del titolare e degli eventuali responsabili, e contenente, tra gli altri, le finalità del trattamento, una descrizione delle categorie di interessati e dei dati personali, i destinatari, gli eventuali trasferimenti verso Paesi terzi e una descrizione generale delle misure di sicurezza.

5. Valutare se è necessaria una DPIA

DPIA, acronimo inglese per *Data Protection Impact Assessment,* è una valutazione di impatto sulla protezione dei dati.

La DPIA è obbligatoria solo qualora un trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*

In generale è necessaria condurre una DPIA quando un trattamento soddisfa **due dei criteri di seguito indicati** → *vedi successivo*

Quando prevedere la DPIA?

- **Trattamenti valutativi o di scoring, compresa la profilazione** e attività predittive, in particolare a partire da *“aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”* .

Esempio: una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.

Quando prevedere la DPIA?

- **Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura**: trattamenti finalizzati ad assumere decisioni su interessati che producano *"effetti giuridici sulla persona fisica"* ovvero che *"incidono in modo analogo significativamente su dette persone fisiche"*

Esempio: il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione.

Quando prevedere la DPIA?

- **Monitoraggio sistematico:** trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o *"la sorveglianza sistematica di un'area accessibile al pubblico"*

Esempio: il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione.

Quando prevedere la DPIA?

- **Dati sensibili o dati di natura estremamente personale:** si tratta delle categorie particolari di dati personali oltre ai dati personali relativi a condanne penali o reati.

Si tratta di dati personali considerati sensibili, in quanto connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza) ovvero in quanto incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) ovvero in quanto una loro violazione comporta evidentemente un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

Quando prevedere la DPIA?

- **Trattamenti di dati su larga scala**

- **Combinazione o raffronto di insiemi di dati**, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato.

Quando prevedere la DPIA?

- **Dati relativi a interessati vulnerabili:** la categoria degli interessati vulnerabili comprende anche i minori, i dipendenti e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

Quando prevedere la DPIA?

- **Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative**, come riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via.

- Tutti quei trattamenti che, di per sé, **"impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".**
  Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

6. Implementare i processi per l'esercizio dei diritti dell'interessato

- **Articolo 15 "il diritto di accesso dell'interessato"**
- **Articolo 17 "il diritto all'oblio"**
- **Articolo 18 "diritto di limitazione di trattamento"**
- **Articolo 20 "diritto alla portabilità"**

7. Rivedere le informative sulla privacy

Le informative sulla privacy e sui cookie vanno riviste alla luce del Gdpr. Il linguaggio deve essere chiaro e va spiegato per quali scopi saranno usati i dati, vanno fornite tutte le informazioni relative al titolare del trattamento dei dati, inclusi i contatti per chiedere modifiche o cancellazioni.

Bisogna poi spiegare su quale base vengono forniti quei dati (consenso, un contratto, un legittimo interesse, etc.) e per quanto tempo saranno conservati o secondo quali criteri. Si deve dire se i dati saranno trasferiti verso Paesi terzi, fuori dall'Unione Europea, cosa molto probabile se si usano servizi come social network o mailchimp.

8. Informare della modifica della privacy policy

Comunicare la nuova policy aziendale a tutti i clienti, amministratori di sistemi, dipendenti, collaboratori e fornitori.

Pubblicarla sul sito web.

Adeguare la newsletter.

Chi contattare?

Clarissa Gulotta

Clarissa.gulotta@confagricolturaveneto.it

Tel. 049 8223544