# Privacy. Nuova disciplina a decorrere dal 25 maggio 2018

Il prossimo 25 maggio entrerà in vigore il Regolamento UE n°679/2016 sulla protezione dei dati personali.
Il Regolamento – che è applicabile in tutti gli Stati membri, senza che sia necessario un recepimento nazionale1 - detta nuove norme in materia di privacy, apportando al precedente sistema una serie di importanti novità e inasprendo il sistema sanzionatorio per le violazioni.

## *Misure di accountability. Principio di responsabilizzazione*

Il Regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili, cioè sull'adozione di comportamenti proattivi da parte di tali soggetti tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.
Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative ed alla luce di alcuni criteri specifici indicati nel Regolamento.
Tra i criteri di maggiore rilevanza introdotti nel nuovo quadro normativo dal legislatore europeo vi è il c.d. ***approccio basato sul rischio* (*risk based approach*)**, un approccio nuovo rispetto al Codice della Privacy attualmente in vigore ma non già inedito nel nostro sistema (si pensi alla normativa in tema di Responsabilità Amministrativa degli Enti *ex D.lgs 231/01* ed in tema di Antiriciclaggio *ex D.lgs 231/07*), che traduce in termini concreti il concetto della responsabilizzazione dei titolari nei confronti dei trattamenti da questi effettuati.
In virtù dell'approccio appena ricordato, le misure da adottare in termini di adempimenti Privacy devono essere proporzionali ai rischi effettivamente individuati all'interno della realtà aziendale attraverso *"un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli".*
Si assiste, pertanto, al passaggio da una concezione formale di mero adempimento, ad un approccio sostanziale basato sulla tutela effettiva dei dati e degli interessati; in altri termini, a dispetto della normativa previgente, non sussistono più misure minime da adottare per adempiere agli obblighi Privacy ma, al contrario, spetta al titolare del trattamento dei dati definire gli interventi necessari per adeguarsi alla normativa, con un approccio che garantisca, in buona sostanza, prevenzione ed efficacia.
Assume pertanto importanza la capacità dell'azienda-titolare di individuare e valutare i *"rischi data protection"* (o meglio, gli impatti negativi che un determinato trattamento può causare ai soggetti cui si riferiscono le informazioni) e conseguentemente scegliere le misure atte a mitigarli.

## *Valutazione di impatto privacy (DPIA)*

In tale contesto si inserisce una delle novità della nuova normativa che è data dalla redazione di una "**Valutazione di impatto privacy**"(detta anche DPIA: *Data Privacy Impact Assessment*), ossia di una procedura che descrive il trattamento effettuato per valutarne la necessità, le proporzionalità ed i relativi rischi così da poter adottare misure idonee (in base alla normativa) a gestirli. L'art. 35 del Reg. 679/2016 dispone al riguardo che *"quando un tipo di trattamento … può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".* Il rischio elevato sussiste allorché viene effettuata una valutazione sistematica e globale di aspetti relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondono decisioni che hanno effetti giuridici e significativi sulle persone fisiche; ovvero quando vengono effettuati trattamenti di *"dati particolari"* (gli attuali dati sensibili) su larga scala; ovvero ancora allorché è prevista la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. In sintesi, in considerazione della natura dei dati in possesso delle imprese agricole, e fermi restando gli elementi da considerare nella individuazione del "rischio" che impone l'adozione del DPIA, la configurazione del documento non appare obbligatoria, ma consigliabile, atteso il monito che arriva dal Garante sull'importanza che riveste la redazione dell'atto. Naturalmente riteniamo che la redazione del documento potrà considerarsi non necessaria per quelle imprese che, complessivamente,

abbiano dati estremamente limitati e, soprattutto, non utilizzati per finalità diverse dai soli adempimenti di legge.

***Consenso al trattamento***
La guida del Garante ribadisce che il consenso non è ammesso in modo tacito o presunto e deve essere manifestato attraverso una dichiarazione o un'azione inequivocabile dell'interessato. I contenuti dell'informativa, elencati negli articoli 13 e 14 del Regolamento, sono ampliati rispetto al disposto del Dlgs 196/2003. Se esistenti, vanno sempre specificati i dati di contatto del **RPD-DPO** (Responsabile della protezione dei dati – Data Protecnion Officer). Il titolare deve **specificare un periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione** e il diritto di presentare un reclamo all'autorità di controllo.
Devono inoltre essere esplicitati eventuali processi decisionali automatici attraverso **la profilazione degli interessati**. Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato**, l'informativa dovrà essere fornita non oltre un mese da quando i dati sono stati raccolti**. Il Regolamento fissa inoltre i termini per le risposte da fornire all'interessato, prevedendo che **il titolare deve dare riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego.**

***Registro delle attività di trattamento***
I titolari e i responsabili del trattamento devono tenere un registro delle operazioni di trattamento (i cui contenuti sono indicati all'art. 30 del Regolamento) che, ove richiesto, mettono a disposizione dell'autorità di controllo ai fini dell'eventuale supervisione da parte del Garante.
Vale la pena precisare sin da ora che, il legislatore europeo non pone tale obbligo a carico di imprese o di organizzazioni con meno di 250 dipendenti, salvo che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato ovvero il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati.
Tuttavia, ad onta di tale limitazione, l'autorità di controllo raccomanda tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.

***Misure di sicurezza***
I titolari e i responsabili del trattamento mettono in atto misure tecniche e organizzative adeguate per *"garantire un livello di sicurezza adeguato al rischio"* del trattamento.
Come si evince dalla lettura dell'art. 32 del Regolamento, la valutazione circa le specifiche misure di sicurezza da adottare sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati che derivano, in particolare, dalla distruzione, dalla perdita, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione, di cui rispettivamente agli artt. 40 e 42 del Regolamento, per attestare l'adeguatezza delle misure di sicurezza adottate.

***Notifica delle violazioni di dati personali "Data Breach"***
A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le violazioni dei dati personali2 entro 72 ore dal momento in cui ne vengano a conoscenza e comunque "*senza ingiustificato ritardo*", salvo sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

***Responsabile della protezione dei dati***
In base all'art. 37 del Regolamento, i titolari e responsabili del trattamento sono tenuti a nominare un Responsabile della Protezione dei dati (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer).
In ordine a tale figura, va subito segnalato che la sua nomina è obbligatoria solo in tre casi specifici.

Ciò vale, in particolare, ogniqualvolta il trattamento è effettuato da *autorità pubbliche e soggetti pubblici*, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino *un monitoraggio regolare e sistematico degli interessati su larga scala* ovvero *trattino su larga scala categorie particolari di dati personali.*
Pur tuttavia, è bene evidenziare in questa sede che, anche ove il Regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria.
Rispetto all'istituzione di tale figura (nonché ai requisiti personali e professionali necessari per rivestirla) il Garante ha emanato una specifica FAQ (in aggiunta alle Linee Guida adottate sullo specifico profilo dal Gruppo "Articolo 29") in cui, fermo restando l'elenco dei casi stabilito dal Regolamento comunitario, ha chiarito che la nomina non appare obbligatoria in relazione ai trattamenti effettuati, fra l'altro, da *"imprese individuali o familiari; piccole media imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti"*.

***I nuovi Diritti degli interessati***
Il Legislatore europeo ha introdotto una nuova elencazione (che va dall'art. 15 al 22 del Regolamento) di prerogative riconosciute agli interessati al trattamento, tenendo in considerazione l'attuale sviluppo delle nuove tecnologie che potenzialmente possono determinare nuovi pericoli e rischi per i diritti e le libertà degli stessi. In particolare, tra gli elementi di novità introdotti in termini di diritti degli interessati, meritano un cenno di approfondimento:

- ***Diritto di accesso (art. 15 Reg.)***

Il diritto di accesso si sostanzia nel diritto dell'interessato di richiedere al titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, quindi, di prendere visione o estrarre copia dei vari tipi di documenti a lui riferibili, in applicazione del più generale principio di trasparenza del trattamento dei dati personali.

- ***Diritto alla cancellazione (art. 17 Reg.)***

Il diritto *c.d. "all'oblio*" si configura come diritto dell'interessato di ottenere senza ingiustificato ritardo la cancellazione dei dati personali che lo riguardano, in presenza di uno dei motivi individuati dal Legislatore.

- ***Diritto di limitazione del trattamento (art. 18 Reg.)***

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento previsto dall'attuale disciplina italiana di cui al Codice Privacy.

- ***Diritto alla portabilità dei dati (art. 20 Reg.)***

Si tratta di uno dei nuovi diritti – esercitabile nei casi di trattamenti effettuati con mezzi automatizzati (quindi non si applica agli archivi o registri cartacei) - previsti dal Regolamento all'art. 20, a mente del quale "*L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare cui li ha forniti".*

***Il nuovo sistema sanzionatorio***
Con il Regolamento europeo sulla Privacy sono state inasprite le sanzioni amministrative pecuniarie applicabili in caso di trattamento dei dati personali effettuato in modo non conforme a quanto previsto dalla normativa. Il Regolamento, inoltre, riconosce all'interessato il diritto al risarcimento del danno dal titolare o dal responsabile del trattamento.

## Nota operativa per le imprese agricole

Ciò detto, soffermandoci sulle esigenze delle imprese agricole e su ciò che esse dovranno realizzare in esecuzione dei nuovi obblighi, cerchiamo di fornire dei chiarimenti operativi.
Anzitutto devono essere chiare alcune definizioni:

- **titolare del trattamento**: è qualunque persona fisica o giuridica, autorità o altro che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento dei dati personali;
- **dato personale**: è qualsiasi informazione riguardante una persona fisica identificata o identificabile;
- **trattamento**: è qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di mezzi automatizzati, come la raccolta, la registrazione, la conservazione, l'estrazione, l'uso, la comunicazione, etc., etc.;
- **categorie particolari di dati personali**: sono quelli che il Codice della privacy definisce oggi "dati sensibili", ovvero quelli idonei a rivelare, fra l'altro, l'adesione a sindacati o partiti politici, l'origine razziale o etnica, lo stato di salute di una persona.

Da segnalare quindi che le imprese agricole, nella persona del loro rappresentante ovvero rappresentante legale in caso di società, sono da considerare *"titolari"* ai sensi della normativa privacy.
*"Dati personali"* oggetto della tutela sono **solo** quelli delle persone fisiche, mentre i dati relativi alle persone giuridiche (enti, società, associazioni, consorzi, etc.) non sono oggetto di tutela.
Il Reg. UE n. 679/2016, inoltre, riconosce la figura del **Responsabile del trattamento** (che è la persona fisica o giuridica, l'autorità pubblica o altro che tratta i dati personali per conto del titolare del trattamento).
Detto ciò è da considerare, in linea generale, che le imprese detengono e trattano le seguenti categorie di dati:

- dati del personale impiegato in azienda: comprensivo di tutti coloro che prestano, a qualunque titolo, attività lavorativa subordinata (operai, impiegati, quadri, dirigenti) o autonoma (collaboratori, contoterzisti, etc.);
- dati dei fornitori: tutti coloro che intrattengono rapporti con l'impresa per l'approvvigionamento di beni e/o risorse necessarie allo svolgimento dell'attività;
- dati dei clienti: tutti coloro che intrattengono con l'azienda rapporti commerciali o utilizzo di beni e/o risorse dell'azienda (acquirenti di prodotti, fruitori di agriturismi, etc.).

Come illustrato, il Regolamento UE 679/2016 pone l'accento sulla responsabilizzazione di titolari e responsabili, nel senso che viene affidato ad essi il compito di decidere le modalità, le garanzie ed i limiti del trattamento, nel rispetto dei criteri specifici previsti dal Regolamento.
I principali adempimenti a carico delle imprese agricole si possono ricondurre alla **valutazione della situazione relativa aziendale** (eventuale valutazione di impatto privacy) **e all'informativa per il consenso e alle misure di sicurezza**. Eventualmente va considerata l'opportunità di tenere il **registro dei trattamenti**, obbligatorio per quelle che superano i 250 dipendenti, e la nomina del **responsabile della protezione dei dati**, obbligatoria solo per determinate situazioni.
Coerenti con tali risultanze del Registro dei trattamenti, dovranno essere le informative sulla privacy che l'impresa dovrà fornire a coloro di cui detiene il dato personale ed il conseguente consenso che essi dovranno rilasciare.