FAQ - PRIVACY

(Regolamento Europeo 679/2016 - in vigore dal 25 maggio 2018)

1. **Cos'è il nuovo Regolamento europeo in materia di protezione dei dati personali?**

Il nuovo Regolamento, insieme alla Direttiva in materia di trattamento dati personali nei settori di prevenzione, contrasto e repressione dei crimini, costituisce il ***cd. Pacchetto protezione dati*** approvato dal Parlamento UE il 14 aprile 2016.

Il Regolamento, che offre un quadro di riferimento in termini di *compliance* per la protezione dei dati in Europa, aggiornato e fondato sul principio della responsabilizzazione (*accountability*) si applicherà direttamente a tutti gli Stati Membri a partire dal ***25 maggio 2018***.

2. **Qual è l'ambito di applicazione del nuovo Regolamento?**

Il nuovo Regolamento si applica a tutti coloro che trattano dati personali in maniera automatizzata o non, stabiliti nell'UE o anche extra Ue se le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi a soggetti UE, o il monitoraggio del loro comportamento se tale comportamento ha luogo nell'Unione.

Es. piattaforme web e motori di ricerca saranno soggette al diritto europeo anche se gestite da aziende fuori dall'UE.

3. **Tutti i datori di lavoro al di là del requisito dimensionale devono rispettare il Regolamento?**

Sì. Il Regolamento è rivolto a tutti coloro che trattano *"dati sensibili".*

4. **Come cambia l'*informativa sulla privacy* agli interessati?**

Il Regolamento specifica in maniera dettagliata che l'informativa deve essere scritta, anche con mezzi elettronici, in un linguaggio chiaro, conciso, intellegibile e facilmente accessibile. Può essere fornita oralmente solo su richiesta dell'interessato.

Quanto ai contenuti, vanno sempre indicati**:**

- i dati di contatto del titolare del trattamento e del responsabile del trattamento e del responsabile della protezione dati, se previsti;

- la base giuridica del trattamento, l'interesse legittimo del titolare o di terzi, se costituisce la base giuridica del trattamento;
- l'intenzione del titolare di trasferire i dati personali in Paesi terzi e, se sì, attraverso quali strumenti.

Il Regolamento prevede anche ulteriori informazioni "necessarie per garantire un trattamento corretto e trasparente" (artt. 13 e 14).

5. Quali sono i tempi dell'informativa?

Se i dati sono raccolti presso l'interessato l'informativa va fornita nel momento in cui i dati sono ottenuti (art.13).

Se i dati non sono stati raccolti presso l'interessato l'informativa va fornita al più tardi entro un mese dall'ottenimento degli stessi da parte del titolare (art. 14).

6. Cosa cambia per il consenso da parte dell'interessato?

Per i dati sensibili (art. 9) il consenso deve essere esplicito, lo stesso vale per il consenso a trattamenti automatizzati (cfr. la profilazione - art. 22).

Non deve essere necessariamente prestato per iscritto, ma il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Per questo è consigliabile che sia esplicito, formalizzato e provabile **(scritto).**

Il consenso è revocabile in ogni momento.

Il consenso dei minori è valido a partire dai 16 anni, prima occorre il consenso dei genitori o di chi ne fa le veci.

7. Il consenso raccolto prima del 25 maggio 2018 resta valido?

Sì, se ha le caratteristiche oggi richieste dal Regolamento.

8. Chi è il titolare del trattamento?

È la persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali (art. 4).

Nell'impresa è il titolare dell'impresa.

Negli Enti Bilaterali è il legale rappresentante.

9. Chi sono i contitolari del trattamento?

I contitolari del trattamento sono due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento (art. 26).

10. Chi è il responsabile del trattamento?

È la persona fisica o giuridica che tratta i dati personali per conto del titolare del trattamento (art. 4).

11. Come viene nominato il responsabile del trattamento?

Attraverso un contratto stipulato in forma scritta, anche in formato elettronico, che deve contenere tutte le condizioni del trattamento dei dati e la loro durata, la natura e la finalità del trattamento, il tipo di dati personali, le categorie degli interessati, gli obblighi e i diritti del titolare (art. 28).

Il responsabile può nominare un sub-responsabile per specifiche attività di trattamento (art.28).

12. Chi è il responsabile della protezione dati (RDP-DPO)?

Il soggetto designato dal titolare del trattamento e dal responsabile del trattamento, in alcuni casi specificamente indicati dalla norma (art.37).

Il RDP-DPO può essere un dipendente del titolare o del responsabile del trattamento oppure agire in base ad un contratto di servizi.

13. È obbligatoria la nomina del DPO?

No, ad eccezione delle pubbliche amministrazioni e nel caso di trattamento di dati su larga scala o di trattamento di categorie particolari di dati personali.

Al momento non si ritiene obbligatoria la nomina del DPO nelle piccole e medie imprese del settore.

Per quanto riguarda gli ***Enti bilaterali*** si presume invece che possano sussistere le condizioni per tale nomina, trattando gli stessi dati anche su "larga scala".

14. Cosa si intende per *accountability* di titolari e responsabili? Quali sono i compiti loro affidati?

Si tratta di un'importante novità che si fonda sull'adozione di comportamenti proattivi da parte dei titolari che devono dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

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 e alla luce di alcuni criteri specifici indicati nel Regolamento (art. 23).

15. Cosa si intende per *Data Protection by defalt and by design?*

Si intende la necessità di configurare sistemi e percorsi per il trattamento dei dati sia *ex ante* che *in itinere*, prevedendo quindi sin dall'inizio tutte le garanzie che servono per soddisfare i requisiti del Regolamento.

Si sostanzia nel mettere in atto una serie di misure tecniche e organizzative adeguate e, pertanto, una serie di attività specifiche e dimostrabili da parte dei titolari che devono essere messe in campo prima e durante il trattamento vero e proprio dei dati (art. 25).

16. ## Cosa si intende per *Valutazione d'impatto sulla protezione dei dati*?

Si intende la valutazione che il titolare del trattamento di dati (che può presentare rischi elevati per la libertà e i diritti delle persone fisiche) deve fare, prima di procedere al trattamento, sul rischio dell'eventuale impatto negativo che il trattamento dei dati può avere sulla libertà e sul diritto degli interessati.

All'esito della valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento ovvero consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale (artt. 35 e 36).

17. ## Cosa cambia nel nuovo assetto della tutela della privacy?

L'importante novità è data dal fatto che il titolare del trattamento opera in completa autonomia chiedendo l'eventuale intervento dell'Autorità di controllo solo successivamente, ed eventualmente senza preventive notifiche come avviene oggi.

L'intervento dell'Autorità di controllo sarà, pertanto, un intervento esclusivamente *ex post.*

18. ## Cos'è il Registro dei trattamenti?

Ogni titolare del trattamento e, ove presente, ogni rappresentante tengono un registro delle attività del trattamento svolte sotto la propria responsabilità che deve contenere tutte le informazioni riportate all'art. 30 (tutte le informazioni relative ai dati trattati, ai soggetti coinvolti nella gestione della privacy aziendale, ai tipi di trattamento, alle finalità etc).

Il registro deve essere tenuto in ***forma scritta***, anche in formato elettronico.

Il Garante richiama l'attenzione sulla "sostanziale coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice (Dlgs n. 196/2003) e quelli che devono costituire il registro dei trattamenti".

19. ## Tutti hanno l'obbligo di tenuta del registro?

No. Tale obbligo non è previsto per le imprese e organizzazioni con meno di 250 dipendenti (art. 30), salvo che il trattamento sia un rischio per i diritti e la libertà dell'interessato, che non sia occasionale e che includa dati sensibili, genetici, biometrici giudiziari.

Per le piccole e medie imprese, pertanto, parrebbe non sussistere un obbligo specifico. Ciò non toglie che comunque potrebbe essere prudenziale adottare il registro ai fini della prova di una corretta gestione della privacy.

Diverse le considerazioni da farsi sugli Enti bilaterali a proposito delle quali si daranno opportune informazioni nel prosieguo.

20. ## Quali novità sulle misure di sicurezza?

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento.

Le misure di sicurezza individuate nel Regolamento (art. 32) sono: *pseudonimizzazione, capacità di assicurare riservatezza e integrità del trattamento, procedure per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative*. Tale elencazione è aperta e non esaustiva.

Dopo il 25 maggio 2018 non sussisteranno più obblighi generalizzati di adozione di misure "minime" di sicurezza *secondo quanto previsto dal "vecchio" Codice (art. 33 Dlgs 196/2003)* in quanto la valutazione sarà rimessa, caso per caso, al titolare e al responsabile del trattamento.

Al fine di dimostrare la conformità ai requisiti, richiesti può essere utilizzata l'adozione di codici di condotta (art.40) o di meccanismi di certificazione (art.42), ad oggi ancora non esistenti.

21. Cosa è il Data Breach?

È la violazione dei dati personali che deve essere notificata, in base al nuovo Regolamento, all'Autorità di controllo competente, se possibile, entro 72 ore dal momento in cui il titolare ne sia venuto a conoscenza.

22. Cosa comporta la notifica di una violazione dei dati personali all'Autorità di controllo?

Dal ***25 maggio 2018*** il titolare del trattamento dovrà notificare all'Autorità di controllo, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza, le violazioni di dati personali, salvo che sia improbabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (art.33).

Tali violazioni devono essere comunicate anche all'interessato, senza ingiustificato ritardo.

Il contenuto della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del Regolamento.

23. Cos'è l'Autorità di controllo

Il nuovo Regolamento prevede la costituzione di Autorità di controllo in ciascuno stato membro, rinviando al legislatore nazionale la definizione delle modalità di nomina dei componenti e l'attribuzione di idonee risorse.

L'Autorità di controllo deve sorvegliare l'applicazione del regolamento.

Con il nuovo Regolamento europeo l'Autorità di controllo, che in Italia continuerà ad essere il Garante per la Privacy, interviene principalmente *ex post*, cioè la sua valutazione si colloca successivamente alle valutazioni del titolare del trattamento.

Dal 25 maggio 2018, quindi, saranno aboliti gli istituti quali la notifica preventiva dei trattamenti e il prior checking, sostituiti da obblighi di tenuta di un registro dei trattamenti e da valutazioni di impatto autonome da parte del titolare e dei responsabili.

24.

Cos'è il diritto all'oblio?

Il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.

25.

Cosa è cambiato nelle sanzioni?

Il Regolamento prevede sanzioni molto *importanti* in caso di violazione degli obblighi in materia di privacy.

Il "costo" della mancata *compliance* normativa in materia di privacy ha subito infatti notevoli mutamenti. Le sanzioni oscillano dai 10 milioni di euro fino al 4% del fatturato mondiale dell'impresa o del gruppo.

Mentre le sanzioni penali rimangono di competenza di ogni singolo Stato.

Roma, 18 ottobre 2017

a cura di Bianca Maria Baron e Rossella Messina