

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Regolamento UE 2016/679 del 27 aprile 2016

A cura di:

Marco BOIDI e

Stefania TELESCA





Reg. UE 2016/679 Entrato in vigore il 24 maggio 2016

Il regolamento non ha bisogno di alcun recepimento, ma gli Stati membri hanno **2 anni** di tempo per adeguare le proprie normative interne.

Il nuovo trattamento di protezione dei dati personali abroga la direttiva 95/46/CE e per l'Italia andrà a sostituire l'attuale codice privacy normato dal D.lgs 196/2003.



Diventerà applicabile in tutti i Paesi UE a partire dal **25 maggio 2018**.

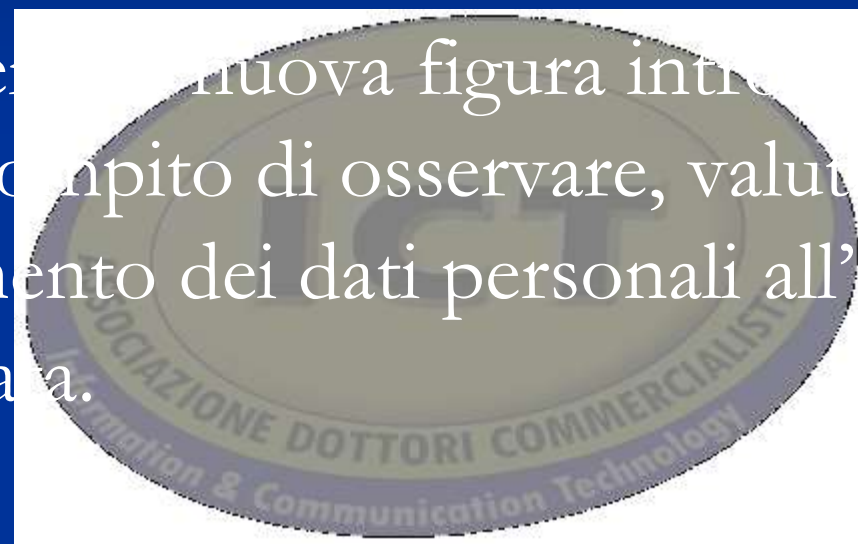
Novità rilevanti

- Diritto all'oblio e rettifica dei dati personali;
- Diritto alla portabilità dei dati;
- Notifica delle violazioni alle autorità nazionali;
- Notifica agli utenti nei casi più gravi di violazione dei dati personali (Data Breach);
- Modalità d'accesso semplificata per consultare i propri dati personali;
- Pseudonimizzazione.



D.P.O.

D.P.O. → Data Protection Officer, nuova figura introdotta dal regolamento 2016/679 che ha il compito di osservare, valutare ed organizzare la gestione del trattamento dei dati personali all'interno dell'azienda, sia pubblica che privata.



La nuova figura professionale va ad aggiungersi ai già noti «titolari», «responsabili» ed «incaricati» del trattamento dei dati personali.

Quando si nomina il D.P.O.?

- Il trattamento è effettuato da autorità pubblica o da un organismo pubblico;
- Le attività principali del «Titolare» o del «Responsabile» del trattamento consistono nel monitoraggio regolare e sistematico degli interessi su larga scala;
- Le attività principali del «Titolare» o del «Responsabile» consistono nel trattamento, su larga scala, di categorie di dati personali di cui all'art. 9 (categorie particolari di dati personali) o di dati relativi a condanne penali e reati di cui all'art. 10.





Art. 9 Reg. UE 2016/679

«E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».



L'art.9, al paragrafo 2, disciplina tutti quei casi in cui è possibile raccogliere gli elementi sopra indicati.

Cos'è la valutazione d'impatto sulla protezione dei dati?

L'art. 35 del presente Regolamento esamina nel dettaglio gli elementi che necessitano di una particolare analisi.

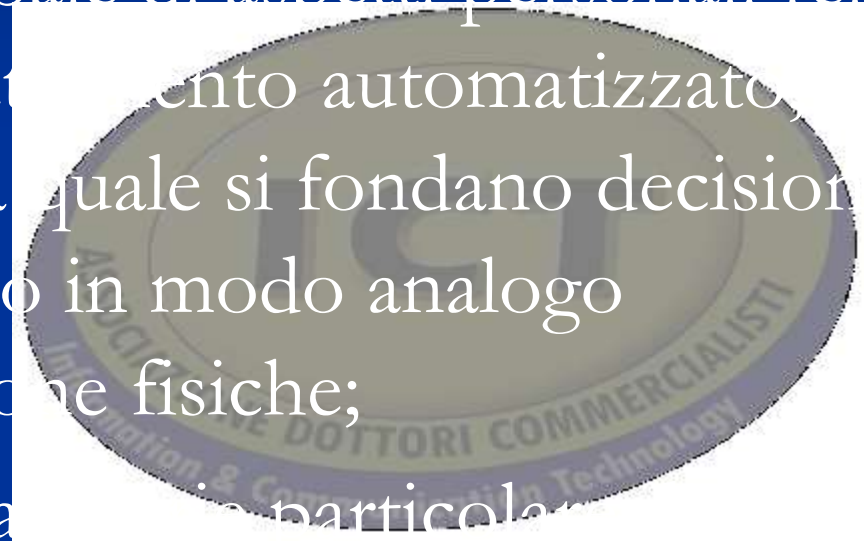


«Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi».



Quando è richiesta la valutazione d'impatto sulla protezione dei dati?

- Una valutazione sistemica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento su larga scala di categorie particolari di dati personali, art. 9 (dati sensibili) art. 10 (giudiziari);
- la sorveglianza sistemica di una zona accessibile al pubblico su larga scala.





Cosa contiene la valutazione d'impatto sulla protezione dei dati?

- Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal responsabile del trattamento.
- Una valutazione delle necessità e delle proporzionalità dei trattamenti in relazione alla finalità.
- Una valutazione dei rischi per i diritti e le libertà degli interessati.
- Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.





Casi di esonero dalla valutazione d'impatto sulla protezione dei dati?

- Esonerate dalla conservazione delle informazioni e dalla valutazione d'impatto sulla protezione dei dati sono le micro, piccole e medie imprese che hanno meno di 250 dipendenti.
- Il Regolamento non si applica al trattamento dei dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale.
- Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato.



Rapporto con accordi precedentemente conclusi

«Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali che comportano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali conclusi dagli Stati membri prima del 24 maggio 2016 e conformi al diritto applicabile in materia di tale modifica».





Proposta Associazione ICT Dott.Com

Effettuare la valutazione d'impatto prima del 2018





Grazie per l'attenzione



Per maggiori informazioni: info@ictdott.com