

Come sta la privacy ad un anno dall'attuazione del GDPR?



Il Regolamento (Ue) 2016/679, noto anche come **RGPD** (Regolamento Generale sulla Protezione dei Dati) o **GDPR** (*General Data Protection Regulation*), troverà piena attuazione esattamente fra un anno da oggi, il **25 maggio 2018**, ovvero al termine del periodo di transizione.

A seguito dell'interessante seminario svoltosi venerdì 19 maggio 2017 presso l'Ordine degli Ingegneri di Bologna sulle **possibili forme di certificazione in ambito Privacy**, è utile fare qualche riflessione sull'attuazione di questa nuova normativa nelle organizzazioni del nostro Paese.

Attualmente esistono alcuni documenti ufficiali che permettono di comprendere meglio come declinare i requisiti del GDPR nella propria organizzazione, tra i quali:

- [Linee Guida all'applicazione del RGPD del Garante Privacy italiano](#)
- [Linee guida sui responsabili della protezione dei dati \(RPD\) WP 243 \(174 download\)](#) (compreso l'allegato con le FAQ)
- [Linee Guida Valutazione-Impatto WP 248 \(212 download\)](#) .

Al momento, però, le indicazioni fornite non sono in grado di fugare tutti i dubbi sull'applicazione del GDPR, anzi!

Il GDPR dà spazio a integrazioni dei requisiti in esso riportati per regolamentare situazioni specifiche per tipo di dati trattati e particolari legislazioni nazionali, sarà compito del Garante Italiano definire eventuali disposizioni integrative che avranno valore di Legge.

Esaminando i concetti principali del GDPR, quali **responsabilizzazione** (*accountability*) del titolare e del responsabile del trattamento, **privacy by design**, **privacy by default**, **valutazione di impatto**, **valutazione dei rischi** e "misure di sicurezza adeguate", è facile individuare molti punti di debolezza di numerose organizzazioni italiane che, per mentalità, non sono abituate ad affrontare il problema della protezione dei dati personali con metodo e come una reale priorità. Per molti vertici aziendali la privacy è "solo una scocciatura" e il nuovo Regolamento un "ennesimo obbligo cui toccherà adeguarsi", ma non tanto prima della scadenza. Come se bastasse fare quattro documenti per risolvere il problema per sempre (o per lo meno fino al prossimo cambiamento normativo)!

Purtroppo questo “approccio” per essere conformi al GDPR deve cambiare, perché è una norma di stampo anglosassone (tipo “*common law*”, a dispetto della Brexit) che richiede una **forte responsabilizzazione di coloro che ricopriranno il ruolo di titolari** (rappresentanti legali per le società) **e responsabili del trattamento**.

L'affidamento all'esterno di dati personali, anche solo per adempimenti legislativi, come la preparazione delle buste paga demandate allo Studio di Consulenza del Lavoro, devono richiedere un'attenta analisi del contratto con il soggetto esterno e verifica che esso soddisfi tutti i requisiti in termini di misure di sicurezza per la protezione dei dati.

Certamente per le PMI che trattano solo dati personali di dipendenti e collaboratori, oltre a nominativi di referenti di clienti e fornitori, l'adeguamento al GDPR non sarà di particolare impatto, ma basta demandare all'esterno ad un servizio via web come la gestione del personale oppure avere un sito internet di *e-commerce* che raccoglie dati di utenti per rendere la gestione un pochino più complessa.

Viceversa le **organizzazioni che trattano dati particolari** (i.e. sensibili), soprattutto se poco strutturate e se gestiscono tali dati insieme a fornitori di servizi mediante internet, dovranno cambiare il loro atteggiamento sulla privacy e valutare attentamente i rischi che corrono. Soprattutto non credano che basti far scrivere un DPS o “riesumere” quello precedentemente redatto prima che il Governo lo abolisse: la carta (o i documenti digitali) non bastano, occorre la consapevolezza e la sostanza di applicazione di regole comportamentali, misure di sicurezza fisica e logica (sistemi informatici) ritenute adeguate (da chi?) e instaurare con fornitori e partner rapporti contrattuali che prendano in considerazione anche il trattamento dei dati personali e la loro tutela.

Recenti eventi come i *ransomware* del tipo *Wannacry* potrebbero far piangere veramente i titolari di trattamenti di dati sanitari, il cui valore per gli hacker potrebbe essere ben superiore dei 300 dollari in Bitcoin. Il ricatto potrebbe essere non del tipo “se riuoi i tuoi dati paga”, ma “se non vuoi che divulghi su internet i tuoi dati paga il riscatto”!. Ci sono stati già casi analoghi legati a ricatti a proprietari di diritti di serie TV americane molto più innocui.

Relativamente al ruolo del DPO, l'obbligo di nomina imposto dal Regolamento ricade in modo certo solo su Enti Pubblici, mentre le Organizzazioni che controllano in modo regolare e sistematico dati personali di interessati su larga scala e quelle che trattano dati particolari (traducibili con i dati sensibili del vecchio Codice Privacy, D.Lgs 196/2003) su larga scala o trattano dati relativi a condanne penali e reati non sono facilmente determinabili. Cosa significa “su larga scala”? Le indicazioni fornite hanno permesso di stabilire che un medico di base della Sanità Italiana non tratta dati sanitari su larga scala, ma come considerare strutture superiori come Farmacie, Ambulatori medici Privati, Cliniche Private? Gli Studi Legali devono nominare un DPO?

Sicuramente le **competenze del DPO** dovrebbero comprendere competenze **legali** (conoscenza di normative e leggi applicabili alla materia ed ai dati trattati dall'organizzazione titolare del trattamento), competenze **informatiche** (non necessariamente particolarmente approfondite, per esse può rivolgersi a tecnici specializzati come sistemisti ed esperti di sicurezza informatica) e **gestionali-organizzative**.

Relativamente alle forme di **certificazione sulla privacy** che, beninteso, non esimono i titolari ed i responsabili del trattamento da essere passibili delle sanzioni previste dal Regolamento e dal Garante Privacy Italiano in caso di infrazioni, occorre distinguere fra diversi tipi di certificazione:

- Certificazione di prodotto o servizio, accreditata secondo ISO 17065, come ad es. lo schema ISDP 10003:2015 – *Criteri e regole di controllo per la Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali – Reg. EU 679/2016*.
- Certificazione delle figure Professionali della Data Protection (DPO, “Auditor Privacy”, “Privacy Officer” e “Consulente Privacy”).
- Certificazione delle Aziende del *Data Protection Management System* in conformità al Codice di Condotta DPMS 44001:2016° ed al Reg. (UE) 679/2016.
- Certificazione del sistema di gestione della sicurezza delle informazioni secondo la ISO 27001:2013.

Premesso che la certificazione accreditata secondo il Regolamento UE 679/2016, così come esposta dall'articolo 43 dello stesso RGPD, trova attualmente riscontri solo in standard e certificazioni afferenti allo schema di accreditamento ISO 17065 (certificazioni di prodotto o servizio), emergono le seguenti considerazioni:

- Non si è ancora affermato un sistema di gestione della privacy riconosciuto che, sulla base della struttura HLS delle norme sui sistemi di gestione (ISO 9001, ISO 27001, ecc.), consenta di gestire la protezione dei dati con un approccio sistemico, basato sui processi e concetti come il *risk based thinking* e l'attuazione di azioni finalizzate ad affrontare i potenziali rischi sul trattamento di dati personali.
- Il ruolo del *Data Processor Officer* (DPO o RPD), come è definito dal Regolamento, non corrisponde ad una figura professionale specifica avente determinati requisiti di competenza (istruzione scolastica e post scolastica, conoscenze normative e tecniche, esperienza nell'ambito privacy, partecipazione a corsi di formazione, superamento di esami o abilitazioni). Il DPO è piuttosto “un ruolo” che potrebbe richiedere competenze differenti a seconda della realtà in cui opera e della criticità della protezione dei dati personali nell'organizzazione stessa.
- Tutti gli schemi e gli standard sopra indicati permettono di ridurre il rischio che il titolare del trattamento e gli eventuali responsabili incorrano in infrazioni nel trattamento di dati personali e, quindi, rischino infrazioni anche pesanti e/o gravi danni di immagine.

Per concludere, secondo il *risk based thinking*, quali rischi corrono le aziende che non sono adeguate al GDPR?

La probabilità di essere sanzionati a seguito di ispezioni del Nucleo Privacy della GdF è estremamente bassa, un po' più alta per organizzazioni che trattano dati particolarmente critici (la valutazione è fatta in base al numero delle ispezioni avvenute negli ultimi anni).

La probabilità di incorrere in sanzioni o in risarcimento danni a causa di istanze di interessati che si sentono danneggiati nella loro privacy oppure in caso di incidenti di dominio pubblico è un po' più alta.

L'impatto delle conseguenze nel caso si verificano suddetti eventi negativi dipende dal tipo di organizzazione e dai dati trattati, può essere significativo o devastante a seconda dei casi.

Leggi anche l'articolo [Impatti del Regolamento Privacy sullo sviluppo software](#).