Prime esperienze di applicazione del GDPR

Il GDPR è divenuto pienamente attuativo dal 25 maggio scorso, anche se in realtà era stato pubblicato due anni prima, però il processo di adeguamento delle imprese italiane al GDPR è ancora in corso. Questo perché da un lato, come è consuetudine nel nostro Paese, le Imprese affrontano le scadenze legislative solo all'ultimo momento, non preoccupandosi di capire prima quanto tempo è necessario per l'adeguamento legislativo. Dall'altro anche le Istituzioni (Stato Italiano e Garante Privacy) stanno impiegando molto più tempo del previsto per rendere completo, ed auspicabilmente di chiara interpretazione, il panorama legislativo in materia di protezione dei dati personali.

Il fatto che molti punti del GDPR non sono di facile interpretazione e, anzi, gli approcci sono talvolta differenti, non ha fatto altro che rallentare il percorso di adeguamento.

Tra gli effetti collaterali di questo lento percorso di adeguamento c'è la difficoltà di interfacciarsi con i soggetti esterni all'impresa o allo studio professionale, perché il mondo perfetto in cui i miei clienti ed i miei fornitori sono già adeguati al GDPR – e lo hanno interpretato in modo uniforme – al momento non esiste, e non si sa quando ci si arriverà.

Passiamo ad esaminare le principali problematiche – e possibili soluzioni – delle prime applicazioni del GDPR in organizzazioni di diverso tipo e dimensioni.

1) **Informative e consensi**

L’informativa è lo specchietto delle allodole della nuova normativa sulla privacy; non bisogna credere che basta trovare un modello di informativa, magari gratuitamente dal web o da amici e colleghi, per aver risolto il problema privacy: uno su mille ce la fa! Solo pochi singoli (ditte individuali, professionisti singoli) senza dipendenti possono accontentarsi della nuova informativa.

Inoltre, l’informativa ha un contenuto che non può essere redatto in modo completo solo partendo da un modello standard e conoscendo l’art. 13 (e seguenti) del Regolamento UE 679/2016; occorre conoscere come funzionano i flussi di trattamento dei dati personali nell’organizzazione. Magari attraverso un’assessment ed una *gap analysis* approfondita, soprattutto nelle organizzazioni più complesse.

Infine, c’è il problema di come comunicare l’informativa agli interessati. Occorre analizzare bene requisiti normativi, processi gestionali ed esigenze organizzative per scegliere le modalità più opportune. Probabilmente un’informativa pubblicata su una pagina web ed una e-mail ai clienti (effettivi e potenziali) e fornitori, che comunica l’aggiornamento dell’informativa privacy, reperibile al sito www…. è la soluzione migliore nella maggior parte delle organizzazioni, soprattutto se operano B2B.

2) **Responsabili esterni del trattamento**

Il GDPR ci dice di identificare i soggetti esterni all’organizzazione che trattano per “suo conto” dati personali e di designarli come responsabili del trattamento attraverso un atto a valenza contrattuale.

In primo luogo occorre stabilire quali fornitori (e non solo) operano come responsabili del trattamento perché trattano dati personali di cui l’organizzazione è titolare del trattamento: società e studi che forniscono servizi contabili e fiscali,

società e studi che forniscono servizi di elaborazione buste paga e consulenza del lavoro, società che forniscono servizi informatici (servizi di assistenza sistemistica, fornitori di software gestionale ed applicativo, fornitori di servizi cloud, ecc.) sono solo alcuni candidati… occorre anche qui capire come si svolgono le varie attività internamente ed esternamente ed è necessario valutare l'affidabilità del fornitore in termini di garanzie relative alla protezione dei dati personali.

Per gestire correttamente questo punto bisogna essere in due ed essere d'accordo sulla nomina di responsabile del trattamento e sui relativi obblighi contrattuali del responsabile.

Questa attività di "regolarizzazione" dei responsabili del trattamento è spesso lunga e non priva di ostacoli, anche per l'inerzia dei fornitori in questione a rispondere a semplici questionari nei quali si va a chiedere loro quali misure di sicurezza sono state implementate al loro interno (ad es. nella gestione operativa dello studio e/o nel software). Se poi il fornitore non accetta la nomina a responsabile del trattamento (e dei relativi obblighi contrattuali) perché si sente titolare autonomo o semplice soggetto autorizzato a trattare dati personali, ecco che il processo di adeguamento al GDPR si complica enormemente. Se si prende spunto dai sistemi di gestione qualità ISO 9001 si comprende che i fornitori dovranno essere "qualificati" per fornire la nostra organizzazioni e situazioni nelle quali il fornitore tiene "in scacco" il cliente in tema di privacy sono da evitare.

3) **Registro delle attività di trattamento**

È un adempimento non solo formale (praticamente l'unico richiesto alla stragrande maggioranza delle organizzazioni), ma sostanziale: per redigere il registro dei trattamenti (del titolare e del responsabile) bisogna conoscere quali dati personali vengono trattati, in quali processi

dell’organizzazione e con quali modalità. Anche in questo caso occorre un’analisi dei processi dell’organizzazione precisa e puntuale. Effetto collaterale di questa attività di mappatura dei flussi di dati dell’organizzazioni potrebbe essere quello, gradito, di individuare gestioni di dati ridondanti e inefficienti, da eliminare in prospettiva, non solo di privacy.

Ci sono diverse interpretazioni nella composizione del Registro dei trattamenti, francamente non credo che le diverse interpretazioni possano costituire un rischio di *compliance* del registro dei trattamenti a fronte di ispezioni del Garante, dato che in fondo non esistono linee guida chiare sulle corrette modalità di alimentazione dei registri dei trattamenti (le recenti FAQ del Garante in merito non aiutano più di tanto).

Un registro completo anche di informazioni non necessariamente richieste dal GDPR, ma utili nella gestione dei dati personali (es. software gestionali ed applicativi che trattano i dati personali, funzioni aziendali autorizzate a trattare i dati, ecc.) risulta utile per comprendere come sono gestiti i dati personali.

Da ultimo, per completare i registri dei trattamenti occorre sapere per quali attività di trattamento l’organizzazione è titolare del trattamento e per quali è solo responsabile: e ciò si lega alle problematiche del punto precedente, anche in senso opposto, relativamente ai ruoli di titolare e responsabile del trattamento, o magari di contitolare.

4) **Misure di sicurezza tecniche ed organizzative**

La definizione delle misure di sicurezza adeguate è uno dei punti più difficili del GDPR. Propedeutica a questa attività c’è la valutazione dei rischi che incombono sui dati personali e soprattutto sulle persone fisiche cui si riferiscono.

Al di là della criticità o meno dei trattamenti effettuati

dalle diverse organizzazioni occorre stabilire un livello minimo di sicurezza nei sistemi di protezione dei dati personali, coerente con gli standard nazionali ed internazionali e le *best practice* di sicurezza informatica. Il problema è che non esistono più le misure minime di sicurezza stabilite per legge, anche se alcune di esse (non tutte) rimangono valide a livello di standard minimo di sicurezza sostenibile davanti ad un Giudice. Infatti, dobbiamo pensare al caso peggiore: l'ispezione del Nucleo Privacy della Guardia di Finanza (magari a seguito di un *data breach*) e le richieste di risarcimento danni di un interessato che si ritiene danneggiato da una violazione dei suoi dati personali.

Allora occorre documentare lo stato dei sistemi informatici con riferimento alle misure di sicurezza implementate e documentare anche le misure organizzative attuare. È il minimo per dimostrare *l'accountability*, ma può essere solo un punto di partenza se le misure implementate non sono convincenti per essere sostenute nei confronti di terzi.

Nelle PMI talvolta la gestione sistemistica dei sistemi informatici è delegata ad un soggetto esterno (singolo professionista o società di servizi informatici). In questi casi il titolare dei trattamenti come minimo dovrebbe pretendere una descrizione dettagliata delle logiche di funzionamento dei sistemi e delle misure di sicurezza implementate, ma spesso il fornitore è restio a documentare una prassi non completamente sicura, implicitamente accettata dalla Direzione aziendale che non intendeva sobbarcarsi ulteriori costi per rendere maggiormente sicuri i sistemi.

Una misura di sicurezza (organizzativa) è costituita proprio dalla disponibilità di relazioni e dichiarazioni scritte da parte del fornitore di servizi IT.

Tra le misure organizzative di sicurezza rientrano anche nomine ad amministratore di sistema (secondo il provvedimento del Garante per la Privacy del 2008 ancora valido) di coloro

che di fatto svolgono tali mansioni, contratti con fornitori che garantiscono sicurezze adeguate sui dati personali da essi gestiti, compresa una designazione a responsabile esterno del trattamento, la formazione del personale, procedure e istruzioni interne.

Su quest'ultimo aspetto risulta molto utile istituire una sorta di "Regolamento informatico interno", che descriva le regole da seguire da parte del personale quando utilizza i dispositivi ITC messi a disposizione dall'azienda e non solo. Tale Regolamento dovrebbe trattare – coerentemente con le misure di sicurezza effettivamente implementate – argomenti quali: gestione delle password, gestione delle postazioni di lavoro, gestione dei dispositivi portatili, misure di sicurezza da adottare in viaggio, modalità di utilizzo dei dispositivi elettronici assegnati (cosa si può fare e cosa no), regole da seguire nella navigazione internet e nell'utilizzo della posta elettronica e così via.

Tali disposizioni, oltre che per la protezione dei dati personali, sono utili alla Direzione aziendale per garantirsi in caso di atti illeciti commessi da un dipendente tramite strumenti ICT dell'azienda.

Tornando alle misure di sicurezza informatica implementate, le principali carenze che si rilevano, soprattutto nelle piccole e microimprese, sono legate all'utilizzo di antivirus *free* (che talvolta non lo sono per utilizzo a fini commerciali), indirizzi di posta elettronica gratuiti, piattaforme in cloud gratuite, servizi di trasmissione di file di grandi dimensioni, ecc. Come noto il termine "gratis" è estremamente gradito a molti piccoli imprenditori, ma per chi tratta dati personali, specie se di tipo sanitario o giudiziario, i sistemi gratuiti offerti anche da importanti *player* mondiali quali Google, Microsoft, ecc. potrebbero non rappresentare una misura di sicurezza adeguata. Se i dati personali sono critici dal punto di vista della riservatezza, sistemi che non la garantiscono a priori (il servizio gratuito è generalmente

fornito in cambio dell’utilizzo dei dati) non costituiscono la scelta migliore. Inoltre la conservazione di dati personali in *cloud storage* che fisicamente risiedono fuori dalla UE è ammessa solo sotto determinate condizioni.