LA DPIA

Data Protection Impact Analysis

a cura di ING. N. CASTELLITI
visto da: ING. P. ROCCO, ING. M. NAVA
Commissione SICUREZZA INFORMATICA

LA DPIA

Data Protection Impact Analysis

a cura di ING. N. CASTELLITI
visto da: ING. P. ROCCO, ING. M. NAVA
Commissione SICUREZZA INFORMATICA

Introduzione

Il nuovo Regolamento 679/2016 sulla protezione dei dati personali sarà completamente operativo il 25 maggio 2018, prendendo il posto dell'attuale Codice Privacy, D.Lgs. 196/2003. Leggendo la versione inglese del Regolamento ci si rende conto che, salvo una nota incidentale, il termine "privacy" non viene mai menzionato, a riprova del fatto che si sta traghettando da un concetto di protezione della privacy a quello più prosaico e misurabile della protezione del dato personale, con il fine di favorirne la libera circolazione. A parte questa precisazione, sono diverse le affinità del Regolamento con la nostra legge 196. In particolare i principi di liceità, correttezza e trasparenza nei confronti dell'interessato sono sempre alla base del trattamento così come la chiara definizione della finalità sulla quale si basa il consenso.

Una delle principali differenze fra i due impianti legislativi è la modalità offerta per la risoluzione delle situazioni che più espongono al rischio di un trattamento scorretto. Il Codice parla di "misure minime", termine con cui si intende "il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti…"; in altre parole mette a disposizione uno strumento di lavoro (Allegato B) al quale attenersi per poter garantire un livello di sicurezza formale e sostanziale orientata a mantenere sufficientemente bassa l'esposizione al rischio. Il Regolamento invece fa spesso menzione di "misure ragionevoli", termine col quale delega al Titolare del trattamento la responsabilità della decisione sull'idoneità delle misure in base a parametri quali la natura del dato, la modalità del trattamento, l'accessibilità alle tecnologie; in altre parole delega la responsabilità della DPIA.

Quando effettuare la valutazione d'impatto sulla protezione dei dati (DPIA)

E' il metodo cardine con il quale il Regolamento assegna la responsabilità al Titolare nel decidere se il trattamento è suscettibile di rischio. Il primo comma dell'articolo 35 recita: "*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.*"

Al fine di decidere il grado di esposizione al rischio del trattamento e conseguentemente l'opportunità di svolgere una DPIA, viene in aiuto il documento WP248 dello *European Data Protec-*

tion Board (ex Working Party) nella versione emendata ed adottata il 4 ottobre 2017. Questo suggerisce di prendere in considerazione i seguenti nove criteri:

1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive
2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura
3. Monitoraggio sistematico
4. Dati sensibili o dati di natura estremamente personale
5. Trattamenti di dati su larga scala
6. Combinazione o raffronto di insiemi di dati
7. Dati relativi a interessati vulnerabili
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
9. Tutti quei trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto" (segue definizione di "monitoraggio sistematico" e "larga scala")

Nella maggioranza dei casi un Titolare del trattamento dei dati personali può ritenere opportuno svolgere una DPIA quando almeno due delle casistiche sopra esposte vengono soddisfatte.

Come realizzare la valutazione d'impatto sulla protezione dei dati

Fare una DPIA significa effettuare un'analisi del rischio. Si possono adottare diverse tecniche, qualitative e quantitative, al fine di valutare il rischio in un processo sotto l'aspetto della protezione del dato personale trattato. Uno dei metodi più comuni è l'FMEA, *Failure Mode and Effect Analysis* (Analisi dei modi e degli effetti dei guasti). Questo strumento permette di valutare il rischio come prodotto di tre indici:

Severità
: Stima della gravità di un evento, opportunamente indicizzata e misurabile

Occorrenza
: Stima della frequenza possibile di accadimento, opportunamente indicizzata e misurabile

Rilevabilità
: Stima della capacità del sistema di rilevare un evento rischioso e farvi fronte

Definito lo strumento, si passa ad identificare le categorie degli eventi che rappresentano un potenziale rischio per il trattamento in oggetto. Questa fase è fortemente collegata agli aspetti precipui del trattamento, del contesto aziendale, delle persone e loro formazione, ecc… Gestire l'elenco dei clienti di un laboratorio di analisi o di un'azienda di apparecchiature biomediche potrebbe essere più complesso e rischioso dell'anagrafe degli iscritti di una palestra. Ad ogni modo per avere un supporto nella definizione della tassonomia degli eventi di rischio, è consigliabile ricondursi a standard riconosciuti da cui poi dettagliare i singoli eventi caso per caso. Vengono in aiuto, da questo punto di vista, oltre allo stesso GDPR, la ISO27001 - Sistemi di gestione della sicurezza delle informazioni - e la 29134 – Linea guida per una Privacy Impact Assessment.

In figura 1 viene presentata una possibile tassonomia di aree/funzioni investigate che si possono ricondurre a sei processi che ne formano una sintesi. Ad ogni riga può essere associato uno o più eventi potenzialmente rischiosi da valutare con la tripletta di indici definiti sopra. In figura 2 si presenta uno spaccato di uno studio sul trattamento dei dati gestiti dal ciclo attivo di un Customer Service.

Calcolata la media dei rischi per processo, se ne può presentare una sintesi con un diagramma spider come in figura 3. La linea azzurra rappresenta lo stato di rilevazione iniziale, quella rossa uno stadio intermedio o finale che tenga conto di un processo di gap analisi e piano di rientro. Occorre sottolineare che l'analisi e l'abbattimento del rischio tengono conto dell'evoluzione dell'organizzazione: si tratta, quindi, di un processo dinamico.

In questa fase si cerca di rilevare opportuni attributi che possano descrivere bene il rischio che si sta trattando al fine di poterlo affrontare meglio, catalogare, quantificare. Ad esempio si definisce quali sono le funzioni aziendali impattate, chi potrebbe essere il responsabile dell'attività di rientro, se il rischio è di origine interna all'organizzazione o esterna ed altro ancora.

Consultazione preventiva per la valutazione d'impatto sulla protezione dei dati

In figura 4 viene presentato il tipico andamento qualitativo del rientro del rischio nel corso degli investimenti ad esso dedicati. In fase di rientro, il livello di sicurezza aumenta velocemente a fronte dei primi investimenti (smart goal). Con il crescere degli investimenti si riduce progressivamente il va-

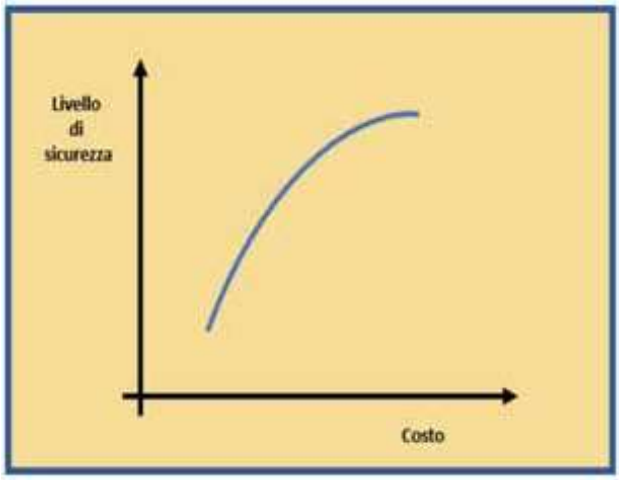
Figura 1

Processo	Funzione investigata
Flusso Trattamento	Acquisizione dato
Flusso Trattamento	Destinazione dato
Flusso Trattamento	Storage
Flusso Trattamento	Backup
Flusso Trattamento	Cancellazione dato
Flusso Trattamento	Dati gestiti all'esterno
Flusso Trattamento	Flussi di dati extra UE
Flusso Trattamento	Dati su internet
Flusso Trattamento	Log di sistema
Documentazione Privacy	Finalità
Documentazione Privacy	Informativa
Documentazione Privacy	Consenso
Documentazione Privacy	Nomine a Responsabile / Persona autorizzata al trattamento dei dati personali / DPO / Rappresentante
Documentazione Privacy	Nomina ad Amministratore di sistema
Documentazione Privacy	Procedure aziendali riguardanti privacy e sicurezza fisica e informatica
Documentazione Privacy	Crisi / Data breach
Asset	Sicurezza fisica delle sedi dove viene effettuato il trattamento
Asset	Infrastrutture di sede
Asset	Rete e trasmissione dati
Asset	Dispositivi portatili
Asset	Software
Asset	Sito web
Asset	Licenze
Asset	Ciclo di vita del cartaceo
Fornitore	Servizi di sede (office automation, guardiania, pulizie, manutenzioni…)
Fornitore	Infrastrutture in cloud
Fornitore	Dispositivi portatili
Fornitore	Rete e trasmissione dati
Fornitore	Software
Fornitore	Consulenti (medici, consulenti del lavoro, auditor, …)
Accessi ai sistemi	Autenticazione (standard o strong)
Accessi ai sistemi	Autorizzazione utenze per ruoli
Accessi ai sistemi	Accesso di terze parti ai sistemi dell'organizzazione
Risorse umane	Formazione per la protezione dati personali per i responsabili e gli incaricati
Risorse umane	Assenza del personale

Figura 2

Figura 3

Figura 4



lore incrementale del livello di sicurezza raggiunto, fino a rendersi inutilmente oneroso. La scelta del punto in cui fermarsi con gli investimenti ricade esclusivamente sul management aziendale. Chi è abituato a gestire progetti di sicurezza identifica, di solito, il trade off nel punto in cui il costo della sicurezza eguaglia quello del rischio.
In situazioni particolarmente complesse può succedere che sia tecnicamente difficile o oneroso abbassare il rischio a livelli ragionevoli. Nel caso in cui il rischio residuo non dovesse essere giudicato sufficientemente basso da rientrare nei limiti di accettabilità, il GDPR prevede una fase di "consultazione preventiva" con il garante, al fine di riceverne una consulenza sulla modalità di procedere nella situazione ritenuta a rischio. Il garante ha l'obbligo di dare risposta scritta alla richiesta entro 8 settimane, prorogabili di ulteriori 6 settimane in caso di particolare complessità del tema proposto; il suo parere è vincolante.

Conclusioni

L'analisi di impatto e la consultazione preventiva rappresentano un cambiamento fondamentale nel trattamento del rischio nell'ambito della protezione dei dati personali. Con il Codice, tuttora vigente, è obbligatorio inviare l'informativa al Garante in tutti i casi di gestione di dati sensibili. Così facendo il Garante ha finora ricevuto una mole notevole di documentazione sulla quale ha potuto esercitare un controllo molto limitato. Viceversa con il nuovo Regolamento il Garante viene coinvolto solo a valle dell'analisi del rischio, cioè con la consultazione preventiva. In questo modo potrà effettuare un'azione più capillare sia in fase di consultazione che di prevenzione.