Articolo DPO-Webinar 4-vers 3
(R.Bellini, AICA-dicembre 2018)

Le difficoltà dei professionisti incaricati della Protezione dei Dati Personali nelle prime applicazioni del GDPR 679/16

Il DPO e il Privacy Manager sono le due principali figure dei responsabili della Protezione dei dati personali che l'impresa e l'ente pubblico debbono mettere in campo secondo la direttiva europea GDPR 679/16 sulla privacy. Dopo i primi mesi di sperimentazione (il GDPR è entrato in vigore alla fine di maggio di quest'anno) la Palestra del Professionista Digitale di AICA ha voluto dedicare una prima riflessione sulle difficoltà concrete che incontrano i DPO secondo 3 esperti di Privacy Management. Hanno partecipato alla riflessione Giuseppe Mastronardi dell'Università di Bari e presidente di AICA, Filomena Polito Privacy Manager della ASL di Pisa e Presidente di APHIM e Marco Bozzetti, Presidente di AIPSI e editor dell'Osservatorio degli Attacchi Digitali (OAD).

Chi sono e cosa fanno i professionisti della Privacy

Cominciamo ad inquadrare le nuove figure del DPO, del Privacy Manager e del Privacy Specialist, così come vengono descritte dalla recente Norma UNI 11697.

La norma UNI identifica tre figure ben distinte:

- A livello operativo, la figura tecnica di riferimento è quella dello **Specialista della Privacy**, che quindi in molti casi ha una esperienza informatica o come tecnico delle comunicazioni, ma che comunque è un professionista con solide competenze ICT per poter gestire questi dati sempre più digitalizzati, sapendo anche in che modo proteggerli. Ed è una protezione che deve essere fatta adottando una serie di tecniche non banali, dalla crittografia, alle tecniche ASCII e all'uso corretto della firma digitale e così via;
- A livello gestionale viceversa, la figura di riferimento è quella del **Manager della Privacy**, che svolge una attività di coordinamento dei vari tipi di trattamento dei dati generati e gestiti in più reparti, dipartimenti e uffici anche di diversa natura;
- Ad un livello più alto di responsabilità di indirizzo troviamo infine la figura del **DPO-Data Protection Officer**: é una figura di garanzia, terza, che ha il compito sia di controllare la corretta applicazione delle procedure di protezione del dato personale, sia di indirizzare e aiutare la struttura operativa a superare gli ostacoli che si possono incontrare nella applicazione del regolamento

Il DPO e il Privacy Manager lavorano entrambi a supporto dell'Imprenditore o del responsabile della gestione, penalmente responsabile della protezione dei dati personali trattati nel flusso di tutte le attività per la gestione del cliente, del fornitore e del personale delle strutture interne.

Le più importanti competenze del DPO e del Privacy Manager

Entriamo un pò più nel merito delle competenze reali delle due figure professionali citate.
Molti DPO hanno una esperienza di gestione della Privacy e della sicurezza informatica. Ma non basta anche se questa è una competenza certamente importante. La sicurezza del sistema informativo è un punto di partenza, ma la sicurezza va resa esecutiva sia sui vari data base che sui flussi di dati che accompagnano la erogazione dei servizi agli interessati interni ed esterni all'organizzazione. È fondamentale poter monitorare gli input e gli output sulla rete di comunicazione con i vari stakeholder connessi , identificando i provider di dati e i poli di

elaborazione e di uso. La sicurezza richiede, ad esempio, che se i dati sono su Cloud, vada chiarito dove e presso quale fornitore sono depositati, se siano protetti e come.
L'esperienza dice che DPO e Privacy Manager devono potersi appoggiare ad una mappa che rappresenti dove sono allocati i vari giacimenti di dati, quale sia la loro natura, quali siano i criteri con cui sono accessibili e quali protezioni sono in vigore rispetto a potenziali minacce di accesso e di uso inappropriato o fraudolento. L'architettura dei processi e dei dati va documentata attraverso il Registro dei Processi e dei Dati a cui aggiungere l'Assessment del Rischio per dare luogo al DPIA, (Data Protection Impact Assessment): questo documento ha l'obiettivo di permettere una ricognizione proprio sulle lacune del sistema di protezione in essere e di facilitare il tracciamento di accessi inappropriati e la valutazione della vulnerabilità del sistema di protezione.

Segue la generazione del report della conservazione dei dati e la predisposizione del registro dei trattamenti, dove si devono mappare i flussi di lavoro per generare e mantenere un inventario aggiornato dei dati. L'analisi va completata con quella del sito web, del consenso dei cookie, del come gestire il consenso.

Una fase molto delicata è costituita dalla valutazione del rischio, che risulta particolarmente complessa quando si tratta di un rischio legato ai fornitori di software che generano dati o ancora di più a fornitori di dati, come si riscontra in un numero crescente di casi. La protezione dei dati del sistema del cliente si trasferisce in questi casi al sistema di controllo sulla sicurezza dei fornitori, con la conseguente valutazione dei loro rischi.

La conclusione è che non è facile fare una valutazione attenta degli incidenti e delle violazioni che avvengono. La materia è complessa e incerta, soprattutto per grossi complessi industriali o di servizio o commerciali: chi fa la valutazione deve fare molta attenzione alla responsabilità che assume, perseguibile anche in termini almeno civili.

Mastronardi sottolinea come "il ruolo del DPO comporta competenze multidisciplinari come elemento caratterizzante; dove anche la interazione con il Privacy Manager è molto stretta" per cui va instaurata una sorta di sincronia per facilitare il raggiungimento della conformità rispetto a quanto prevede la norma. Ma è l'effettiva protezione dei dati che costituisce elemento di concretezza del filo conduttore che porta a concludere che l'approccio e la soluzione dei problemi di protezione sono stati in qualche modo risolti e sono solidi e consistenti.

L'importanza della terziarizzazione dei servizi
Il DPO, che spesso è un consulente esterno e deve aiutare il titolare a supervisionare ciò che viene fatto, si focalizza su quattro macro-livelli di competenza: quelle tecniche, sulla sicurezza informatica, quelle legali, quelle organizzative, completate dalla capacità di contestualizzare su una certa struttura organizzativa dell'azienda o dell'ente e sulla sua cultura dall'altra. Il DPO infine è dotato di capacità manageriali e relazionali, dovendo svolgere un'attività che è trasversale a tutte le business unit e le unità organizzative dell'ente.

Nessuna di queste persone può sapere tutto e conoscere tutto. Devono interfacciarsi coi referenti e responsabili interni e soprattutto con chi, ad esempio, le terze parti esterne, perché molti dei trattamenti personali dei dati sono, in quota parte, terziarizzati. Pensiamo al commercialista, pensiamo ai fornitori ICT che supportano, in Cloud, in housing, in hosting, i sistemi proprietari.

Parliamo infine delle sanzioni applicate nel caso di carenze di conformità. Non risultano ancora casi di applicazioni reali: in teoria si tratta comunque di interventi pesanti, soprattutto per piccole e micro

imprese. Rifacciamoci alla esperienza fata con la Privacy da quando 22 ani fa è entrata in vigore la 196. Quindi non dovrebbe essere qualcosa di nuovo: chi avesse correttamente espletato le norme del precedente codice della Privacy, non avrebbe poi così tanto da fare ancora.

Emergono alcuni aspetti critici della maglia di protezione che in teoria l'organizzazione dovrebbe avere: il discorso è che il GDPR focalizza quattro tipi di misure per la sicurezza, soprattutto per la sicurezza digitale, di tipo tecnico-organizzativo. Uno, impone l'analisi dei rischi: ma questo era richiesto anche in precedenza. E non puoi fare un piano di intervento di sicurezza digitale, se non hai un minimo di idea di quali sono i tuoi rischi e i punti di forza e debolezza del tuo sistema informatico.

Altri aspetti delicati sono: quello dell'accountability, che significa la responsabilizzazione di tutti gli attori: che vuole dire che non solo devi fare le cose e cercare di farle al meglio in maniera efficace ed efficiente, ma devi anche documentarle, perché in caso di ispezione devi dimostrare di avere fatto effettivamente gli interventi previsti. Questo è il primo check di qualsiasi ispezione. Sarà un aspetto burocratico, ma se non c'è quello, si cade ai primi controlli.

Il secondo punto, nuovo rispetto a quanto indicato fino ad oggi nelle precedenti normative sulla privacy, è l'obbligatorietà della segnalazione di un Data Breach subìto (per data breach si intende la **violazione di sicurezza** che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati), cioè se è stato subìto un attacco, con manipolazione o furto dei dati personali con l'obbligo di informare sia le autorità competenti sia gli interessati, eventualmente coinvolti. L'unico modo perché la legge che il GDPR esplicitamente richiama, per evitare questo, cioè di informare poi tutti gli interessati, in alcuni casi è una cosa estremamente impegnativa e di grandissima perdita d'immagine. Si può contrastare criptando i dati personali: arriviamo all' unico effettivo mezzo per il data loss prevention, per proteggere i dati. Che sono il vero asset, soprattutto se sono dati personali. Le tecniche sono consolidatissime, ma la loro messa in opera comporta un aumento della complessità nella gestione dei dati, delle chiavi e dei certificati.

Ci sono delle specificità per quanto riguarda la protezione dei dati personali nel settore della sanità?

Polito ci aiuta a capire meglio quali sono le specificità della protezione dei dati personali nel settore della sanità. Nel merito la figura del Data Protection Officer in ambito sanitario "è caratterizzata dalla necessità di conoscere tutte le altre normative comunque vigenti, da tenere in linea con quella sulla protezione dei dati personali. È importante sottolineare che chi si applica a questa funzione in ambito sanitario svolge una funzione di alta complessità: ci sono infatti nel sistema sanitario molte tipologie di trattamento che dal punto di vista del management, rendono il sistema sanitario una delle amministrazioni più ramificate sul territorio".

Un'amministrazione sanitaria che, anche se privata, risponde a logiche pubbliche, in cui anche i liberi professionisti, rispondono, nel loro operato e negli atti che sottoscrivono, a particolari requisiti di valore medico legale. E questo va tenuto di conto nelle indicazioni che vanno fornite come DPO agli operatori e al management delle aziende sanitarie. Le aziende sanitarie costituiscono quindi un sistema più complesso rispetto alle organizzazioni di altri settori di attività, dove far arrivare la voce del Data Protection Officer. Che d'altra parte deve anche osservare non solo il GDPR, ma anche tutta quella parte della 196 novellata dal decreto legislativo 101, appena entrato in vigore e che rimane comunque vigente".

Anche per chi sia già sia certificato 11697 come Data Protection Officer, la norma però non comprende competenze per profili specifici in ambito sanitario. Quindi, va benissimo come norma che possa dimostrare delle competenze acquisite, ma non differenzia un tipo di DPO dall'altro.

In conclusione, ci troviamo davanti alla indicazione che comunque c'è un grande lavoro ancora da fare in termini di stabilizzazione di quelle che sono le competenze da una parte, ma anche le modalità operative che comunque dovrebbero informare, da una parte, un buon DPO, ma dall'altra anche un buon Privacy Manager. In particolare, suggerisce Bozzetti, dobbiamo "sviluppare la capacità di contestualizzare". Effettivamente il contesto informatico che comprende sia processi che il trattamenti dati in ambito sanitario, è qualcosa di specifico e totalmente diverso. Come sono profondamente diversi gli ambiti di tipo manifatturiero come a sua volta questo differisce dal settore petrolifero o dalla produzione di semi-laminati. Anche se ci sono sempre delle parti simili per ogni contesto è sicuramente vero che i vari DPO si dovranno, più o meno, specializzare per tipologia di contesto. Un conto è l'ambito sanitario, un conto è l'ambito finanziario, un conto è un ambito industriale, un altro è un ambito di servizi".