Come gestire le violazioni di dati personali in azienda secondo il GDPR

Di Andrea Puligheddu – ***Avvocato - Partner Studio Legale Privacy by Orlandi&Partners (www.studiolegaleprivacy.com) - Socio Centro Studi PNT (www.centrostudipnt.org)***

Gestire una violazione di dati personali (aka: *data breach*) non è qualcosa che si può improvvisare.
Come sappiamo l'introduzione dell'obbligo di gestione delle violazioni di dati personali previsto dall'art. 30 del Reg. UE 2016/279 (GDPR) ha comportato un considerevole impatto nei processi organizzativi interni ad aziende ed Enti pubblici.
E le conseguenze di quest'impatto, dal maggio 2018 a oggi si sono viste sia rispetto al mutamento delle procedure che alla corrispettiva mole di sanzioni elevata dall'Autorità Garante per la protezione dei dati personali.

Se infatti pare relativamente esiguo il numero di violazioni riscontrate a titolo di data breach (la più significativa delle quali è rappresentata dalla ordinanza ingiunzione nei confronti di Unicredit S.p.a.), è altrettanto vero che nella loro mole (oltre 650.000 euro e numerosi provvedimenti prescrittivi) esse rappresentano un importante passo in avanti nella diffusione di una cultura privacy condivisa.
Eppure non sono poche le richieste di chiarimento o le gravi confusioni a cui vanno incontro CTO, IT Manager o chiunque sia investito, in ragione del proprio ruolo, del compito di far fronte alle violazioni.
Proprio per questa ragione proviamo in qualche modo ad andare a fondo della questione.
La corretta gestione di un data breach richiede essenzialmente tre elementi:

1. **Visione**
2. **Tempestività**
3. **Crescita**

Visione

La visione concerne la concreta capacità dell'azienda di poter prevedere gli eventuali scenari di rischio. È necessario calarsi in un'ottica di gestione delle emergenze, seguendo un percorso preciso di assessment delle non conformità o delle possibili vulnerabilità. In tal senso uno strumento molto utile che abbiamo riscontrato nella nostra esperienza è proprio l'esecuzione di un *vulnerability assessment* che identifichi con chiarezza le possibili anomalie a livello infrastrutturale, di rete o di software. Tale operazione ha come esito una vera e propria mappa d'azione, che permette all'azienda o all'Ente di portare all'attenzione del board i fattori di rischio e le relative procedure e metodologie di risoluzione. Tutto ciò dovrà poi trovare spazio adeguato nella costruzione di una *data breach policy*, debitamente diffusa all'interno dell'azienda anche attraverso formazione dedicata.
È un lavoro costante, da aggiornare periodicamente, che vive della vita stessa dell'Organizzazione.

Tempestività

Non c'è bisogno di troppe parole quando si viene a conoscenza di un data breach, dato che la chiave di volta nella sua gestione è la rapidità.
Oltre ai termini previsti dal GDPR in tal senso (segnalazione entro 72h o senza indebito ritardo a seconda che si rivesta il ruolo di Titolare o Responsabile del trattamento) occorre considerare le varie ingerenze che potrebbero provenire da soggetti esterni all'organizzazione privacy del titolare:

fornitori, utenti e partner, anche nel caso in cui non siano stati coinvolti dall'eventuale violazione, posseggono i propri ritmi e scadenze. E bisogna tenere in seria considerazione anche il loro impatto nella gestione dell'intera situazione.

Si pensi ad esempio al caso in cui un fornitore di servizi di prenotazione sanitaria online subisca un blocco interno dei server di backup interno, contenente solo DB di sviluppo o di controllo fi gestione, privi pertanto di dati personali diversi da quelli dei dipendenti dell'azienda o al più di alcuni dei fornitori. Il servizio fornito dalla Società dovrà regolarmente essere reso senza interruzioni, ma al tempo stesso potrebbe subire delle anomalie nella sua erogazione dovute alla sovrapposta gestione delle problematiche interne.

Crescita

Una volta passata la tempesta, inizia il vero lavoro.

Si perché limitarsi a gestire un data breach "*rammendando*" i buchi non porterà che una cosa soltanto: la certezza di una prossima violazione.

Per poter correttamente aumentare la security by design dell'Organizzazione è fondamentale crescere nella consapevolezza dei propri limiti e correggerli.

Ecco perché occorre impostare delle procedure (informatiche, ove possibile) di testing periodico dell'infrastruttura per verificare la corretta risoluzione della problematica da cui ha avuto origine il data breach. Ed ecco perché è parimenti importante la formazione costante del personale, basando le proprie docenze a partire dal case history aziendale.

È innanzitutto una questione culturale.

E' chiaro che ogni caso sia da considerare come a sé stante. Per esempio, potrebbe rivelarsi decisivo prendere in considerazione il fattore tempo o ambiente in alcune realtà più di altre, oppure prestare attenzione particolare ai soggetti coinvolti partendo dagli stessi fornitori individuati con apposito contratto di nomina. Nel mondo sanitario, tanto per citare un caso critico, il contesto gioca quasi sempre un ruolo fondamentale nel definire la gravità della situazione, unitamente alla rapidità di presa in carico della violazione e alla tempestiva reazione verso gli interessati.

Per questo c'è sempre bisogno di una valutazione e un affiancamento dedicato, sia da parte del DPO che da altre tipologie di soggetti coinvolti, i quali insieme a un processo collaudato che come Studio abbiamo avuto più volte modo di testare sul campo, potranno portare ad un considerevole abbattimento del rischio in fase di individuazione, gestione e correzione delle violazioni.