Mario Petrulli

Mario Petrulli è avvocato, esperto in edilizia e urbanistica

L'ANALISI DEI RISCHI NEL TRATTAMENTO DEI DATI PERSONALI: UNA BREVE GUIDA

Ormai da alcuni mesi è entrato in vigore il nuovo regolamento europeo sulla privacy n. 2016/679 ed ha obbligato le aziende a rivedere la propria organizzazione ed adottare una serie di misure a tutela dei dati dei propri clienti e, in definitiva, anche a tutela della propria attività. È evidente che la materia necessiterebbe di un approfondimento non possibile in questa sede per comprensibili motivi. Perciò, allo scopo di fornire alcuni elementi di utilità, ci soffermeremo brevemente sull'analisi dei rischi connessi al trattamento dei dati.
Sebbene tale analisi debba considerarsi attività specialistica che richiede il possesso di adeguate nozioni e competenze e, conseguentemente, ogni azienda dovrà opportunamente valutare di affidarsi ad operatori dotati della necessaria esperienza e degli strumenti idonei, è comunque possibile procedere ad una prima analisi semplificata, che ben può rappresentare la base di partenza per una valutazione ben più ampia ed esaustiva.

Prima di procedere, è necessario ricordare alcuni punti essenziali:

- il rischio è, ai nostri fini, il prodotto della frequenza di accadimento e della gravità delle conseguenze;
- poiché i rischi non sono tutti uguali, è necessario prevedere una scala di valori ed associare a rischi maggiori misure sempre più importanti;
- le misure sono rappresentate da quelle azioni che servono a minimizzare i rischi e/o i danni.

Una possibile matrice dei rischi per gli archivi informatici
Tanto premesso, indichiamo di seguito una matrice dei rischi che, sebbene di impostazione semplice, è comunque efficace nell'evidenziare il metodo da utilizzare nell'analisi da parte dell'imprenditore:

PROBLEMA	ELEMENTI DI DEBOLEZZA	DANNI	MISURE
Sottrazione delle credenziali per via telematica	Scarse misure di sicurezza Insufficiente formazione del personale	Accesso illegittimo e conseguente utilizzo di dati da parte di terzi Alterazione e/o distruzione dei dati	Formazione del personale Software ed hardware adeguati Procedure per la corretta conservazione delle password e la relativa modifica periodica
Errore materiale	Insufficiente formazione del personale	Accesso da parte di terzi non autorizzati Alterazione e/o distruzione di dati	Formazione del personale
Virus informatici	Software non aggiornati	Accesso da parte di terzi non autorizzati Alterazione e/o distruzione di dati	Formazione del personale Utilizzo di software periodicamente aggiornati: antivirus, firewall
Hardware e software obsoleti	Scarsa protezione ed efficienza Malfunzionamenti	Problemi di accesso Perdita dei dati	Utilizzo di hardware adeguati e software aggiornati
Accesso fisico da parte di terzi presso i locali interessati	Scarse misure antiintrusione	Furto dei dati	Installazione misure di sicurezza (ad esempio: videosorveglianza, portoncino di ingresso blindato, finestre con sistema anti-intrusione, sistema di allarme) Regolamentazione degli accessi Utilizzo di armadi blindati/ignifughi
Disastri naturali e/o incidenti		Perdita dei dati	Procedure di *disaster recovery*, sistemi antincendio Utilizzo di armadi blindati/ignifughi
Guasto al sistema elettrico		Accesso impossibile Operatività inibita	Gruppo di continuità

Per ciascuna delle aree di rischio (e per quelle ulteriori eventualmente individuate), l'imprenditore dovrà stimare l'indice di rischio, vale a dire la probabilità di accadimento e l'impatto delle conseguenze. Si può, ad esempio, immaginare di individuare quattro livelli:

- rischio basso,
- rischio medio,
- rischio alto,
- rischio altissimo.

Le misure dovranno essere tanto più importanti quanto maggiore è tale livello di rischio.
Inoltre, periodicamente la matrice andrà verificata e, all'occorrenza, opportunamente implementata.

Una possibile matrice dei rischi per gli archivi cartacei
Riprendendo la precedente matrice utilizzata per gli archivi informatici, proponiamo una simile per gli archivi cartacei:

PROBLEMA	ELEMENTI DI DEBOLEZZA	DANNI	MISURE
Errore materiale	Insufficiente formazione del personale	Alterazione e/o distruzione di dati	Formazione del personale
Accesso fisico da parte di terzi presso i locali interessati	Scarse misure antiintrusione	Furto, alterazione e/o distruzione dei dati	Installazione misure di sicurezza (ad esempio: videosorveglianza, portoncino di ingresso blindato, finestre con sistema anti-intrusione, sistema di allarme) Regolamentazione degli accessi Utilizzo di armadi blindati/ignifughi
Disastri naturali e/o incidenti		Perdita dei dati	Procedure di *disaster recovery*, sistemi antincendio Utilizzo di armadi blindati/ignifughi

Le misure di sicurezza

Le misure di sicurezza possono essere classificate, in ragione della loro natura, in tre categorie:

ORGANIZZATIVE	FISICHE	INFORMATICHE
Nomina del responsabile	Sistemi anti-intrusione, di allarme e vigilanza	Utilizzo di username e password per l'accesso ai computer
Rilascio e revoca dell'autorizzazione, da parte del titolare o del responsabile, agli incaricati del trattamento dei dati	Accesso controllato	Password con caratteristiche di sicurezza (di primo accesso con sostituzione obbligatoria da parte dell'utente, numero minimo di caratteri, presenza di lettere, numeri e simboli, blocco dopo 3 tentativi errati, ecc.)
Previsione di diversi livelli di autorizzazione di accesso ai dati in relazione ai compiti e mansioni assegnate	Gruppo di continuità	Periodica modifica della password (ad esempio, ogni 30 giorni) e scadenza dopo non uso prolungato (ad esempio, dopo 90 giorni di inutilizzo)
Verifica periodica delle credenziali di accesso	Sistemi antincendio	Utilizzo di software antivirus, periodicamente aggiornato
Istruzioni scritte per lo svolgimento dei compiti assegnati	Back-up periodico dei dati	Utilizzo di firewall
Verifica della restituzione dei documenti originali al termine delle operazioni affidate	Armadi blindati/ignifughi	Inibizione di accesso a siti considerati non sicuri
Previsione di regole di custodia dei dati da parte degli incaricati durante le operazioni di trattamento		Utilizzo esclusivo di software con licenza
Identificazione e registrazione accessi dopo l'orario di chiusura degli archivi		
Formazione continua del personale		
Verifiche periodiche		
Certificazioni di qualità		
Adesione a codici di condotta		
Aggiornamento periodico della matrice dei rischi ed eventuale implementazione delle misure		
Regolamento interno di condotta