InformatiCH
L'informatica semplice

Guida all'adeguamento normativo LPD
Nuova legge privacy Svizzera.

Via Vallera 16 | 6852 Genestrerio TI | Switzerland | info@informatich.ch

Le fasi

L'adeguamento alla normativa consta di 8 fasi:

- **analisi** del flusso di lavoro;
- **identificazione** dei **trattamenti**;
- **identificazione** delle **persone coinvolte**;
- **nomine**;
- stesura **documentazione**;
- eventuale **adeguamento tecnico**;
- eventuale **adeguamento organizzativo**;
- **formazione** del personale.

Introduzione

Un adeguamento potrebbe anche non coprire tutte le fasi sopra riportate in quanto le aziende, specialmente quando raggiungono una dimensione tale per cui ci siano divisioni in aree di competenza con responsabili e persone adibite a ruoli prestabiliti, tendono ad adottare già naturalmente dei processi aziendali che facilitano l'adozione delle misure tecnico – organizzative richieste dalla legge.

Analisi del flusso di lavoro

Tuttavia è sempre bene compiere *un'analisi approfondita* nella quale *il privato* (così come definito dalla legge, che può essere una ditta individuale, un'azienda oppure un ente pubblico) *collabori* con noi per fornire tutte le informazioni richieste. La fase di analisi passa da *questionari, domande specifiche*, richiesta di visionare documentazione di come sono impostati i *flussi di lavoro* all'interno della realtà esaminata. Una non efficace collaborazione con i nostri incaricati in questa fase potrebbe precludere una buona riuscita del lavoro.

Una volta analizzato il flusso di lavoro, studiando anche i processi aziendali, possiamo procedere a identificare trattamenti e persone coinvolte.

Identificazione dei trattamenti

Ogni privato esiste perché ci sono altri privati o Persone Interessate che lo contattano per acquistare beni e servizi o per richiedere prestazioni istituzionali. **Ogni volta** che avviene una di queste richieste, avviene un **trattamento**. Alcuni vanno protetti, *altri non è necessario che lo siano*.

Tutti questi trattamenti vanno identificati perché per ciascuno è necessario predisporre l'**informativa** prevista dalla legge LPD.

Identificazione delle persone coinvolte

Le **persone coinvolte** sono quelle persone che saranno titolate ad effettuare determinati trattamenti per il privato che è titolare dei dati.

Se poi il privato si avvale di figure esterne per il trattamento di alcuni dati, queste persone saranno da indicare come **responsabili**.

Anche questo passaggio è **fondamentale** per un'informativa di qualità circa la legge LPD.

Nomine

Le persone coinvolte vanno **nominate ufficialmente** in modo che sia **trasparente** e *senza alcun dubbio* la **titolarità** ad eseguire trattamenti sui **dati personali**.

Stesura della documentazione

Bisogna preparare, ed avere sempre a disposizione diversi documenti, tra cui il **registro dei trattamenti**, le **informative**, le **lettere di incarico**, la descrizione delle procedure da attuare in caso di **Data Breach**, ecc.

Eventuale adeguamento tecnico

L'adeguamento tecnico è un passo che va assolutamente affrontato nel caso dell'**adeguamento normativo** alla legge LPD in quanto c'è necessità che vengano adottate **tutte le misure tecniche** che permettono di rispettare quanto **stabilito dalla legge** e deciso da parte del titolare. A scopo esplicativo, non esaustivo e a mero titolo di esempio si citano:

- **compartimentazione** degli accessi;
- **backup**;
- **disaster recovery**;
- **auditing**;
- strumenti di **compliance**.

Da questa fase **potrebbe emergere** che l'infrastruttura del titolare **sia già in regola** con tutti i requisiti, **i TIC** e con tutte le regole di **buon senso**, pertanto non debba essere adeguata. Scaturirà comunque un *documento di descrizione funzionale dell'infrastruttura* che permetterà al titolare di poter **dimostrare** di aver fatto **tutto il possibile** per **tutelare** i dati delle **Persone Interessate** in caso di contestazione.

Eventuale adeguamento organizzativo

Potrebbe emergere, durante l'analisi del flusso di lavoro del Privato, e dall'analisi di tutti i flussi di informazione, che sia **necessario** un **adeguamento organizzativo**, ad esempio per minimizzare il numero di persone coinvolte in un processo in modo da minimizzare il numero di persone coinvolte nel trattamento dei dati. A volte si tratta di rendere **più snelle** e quindi più veloci le **procedure**.

Formazione

Nulla protegge di più da un **Data Breach** della formazione. Le **innovazioni** tecnologiche possono venire in **aiuto** e anche gli **adeguamenti** organizzativi, ma un **personale ben formato** è ciò che **veramente fa la differenza** per i due principi espressi nella legge LPD: **Privacy by Design e Privacy by Default**.

Siamo in grado di **formare** il personale a **comprendere** appieno il perché di certe scelte e il perché, se fino a ieri si procedeva in un modo, da domani si dovrà cambiare modo di lavorare.

Un lavoratore **ben formato** cade molto più **difficilmente** nelle **insidie** moderne per le aziende, dove **il punto debole è diventato l'essere umano**. Verranno date basi per comprendere la normativa, per riconoscere un attacco di **Phishing**, **Spear Phishing**, oppure come accorgersi e difendersi da quegli attacchi in cui viene cercata la **diversione di un flusso di cassa** tramite intercettazione e modifica di fatture, con iban sostituito, per richiedere un pagamento su un conto diverso da quello consueto, intestato all'attaccante o a persone collegate.

Capire quali sono i **rischi** a **scaricare** un programma da **internet**, come gestire l'*ansia di un messaggio urgente* e comunque controllare gli **identificatori di una truffa**, o di un attacco di **Social Engeneering**, queste sono le competenze che miriamo a fornire al personale di chi si affida a noi.