



Obblighi legali

Necessità dell'adeguamento aziendale agli obblighi legali specifici in materia

Aziende coinvolte

Gli obblighi di adeguata analisi dei rischi in ambito privacy e ICT ricadono sull'amministratore di ogni impresa che utilizza sistemi hardware e software ai fini di business

Caratteristiche del servizio

Il servizio copre le tre seguenti aree operative:

1. Adeguatezza dell'assetto organizzativo societario in ambito IT e privacy (artt. 2381 co. 5° e 2043 c.c. e nuovo Regolamento privacy 2016/679).

La governance in area privacy-IT deve risultare ben presidiata (ruoli, deleghe di poteri, nomine, ecc.), gestita in ottica strutturata e continua e non solo come adempimento burocratico. Il soggetto delegante (es. CdA) è chiamato a focalizzare i temi operativi su cui dovrà vigilare successivamente e i soggetti delegati dovranno comprendere chiaramente l'oggetto del successivo reporting.

La privacy può inoltre servire ad ottimizzare alcuni fondamentali processi operativi (es. in area IT+Sales+Legal). Offriamo strumenti che facilitano tali attività di miglioramento.

L'analisi dello stato delle procedure e misure organizzative in ambito privacy-IT e dei rischi correlati va aggiornata periodicamente e coordinata con le valutazioni di adeguatezza organizzativa (art. 2381 co. 5 c.c.) evitando di procedere "a silos". Essa è il punto di partenza per quantificare e misurare gli obblighi tecnico-legali privacy e IT da gestire (i requisiti tecnico-legali di conformità privacy sono davvero molti e il rischio informatico muta nel tempo). Le sanzioni penali, civili, amministrative, in caso di omissioni sono rilevanti.

Il nuovo Regolamento privacy 2016/679 ribadisce l'obbligo di adottare entro il 25 maggio 2018 un approccio organizzativo adeguato in area privacy-IT: in realtà tale obbligo in capo all'impresa non è mai cessato ma viene espressamente ribadito anche per il futuro.

2. Documento Programmatico sulla Sicurezza (DPS)

Il 31 marzo di ogni anno, nella prassi, scade il termine per l'aggiornamento periodico del DPS. L'obbligo di DPS vige da sempre a titolo di misura "adeguata" (in base alle concrete caratteristiche dimensionali, vedi artt. 2381 co. 5° e 2043 codice civile e nuovo Regolamento UE 2016/679 privacy).

Deve pertanto esistere un documento "master" che disciplini tutti i vari adempimenti privacy (non solo informatici ma anche organizzativi e legali) e ne consenta il monitoraggio periodico, al fine di intercettare eventuali scostamenti dalla normativa.

L'azienda deve quindi essere aggiornata e proattiva ed è necessario comprendere quali sono le priorità in termini di rischio e di sanzioni e implementare periodiche modifiche del DPS.

3. Cookies e privacy dei siti web ed attività di e-commerce

Nonostante i ripetuti chiarimenti ed avvertimenti del Garante Privacy, le informative sui cookies e sulla privacy pubblicate sui siti web aziendali sono spesso inesatte o incomplete. Secondo un'indagine Federprivacy del 2016, oltre il 35% dei siti web italiani non è a norma.

Risulta quindi fondamentale verificare se, e come, il webmaster ha garantito la conformità del sito alla normativa privacy. Alcuni tool in commercio risultano non adeguati allo scopo. E' d'obbligo accertare se i testi utilizzati siano completi e allineati alle best practices legali e che tutte le funzionalità tecniche del sito web siano legalmente conformi. Nel caso di attività di e-commerce, inoltre, il sito dovrà rispettare ulteriori specifiche normative.

In caso di inadempimento vi sono pesanti sanzioni (da 6.000 a 120.000 euro in base al tipo di violazione) e si rischiano danni reputazionali e azioni risarcitorie da parte degli utenti interessati.

Il nuovo Regolamento UE Privacy 2016/679 è l'occasione per adeguarsi a quanto sopra.

Contatti

Adacta Studio Associato

www.adacta.it | T. +39 0444.228000

l.demuri@adacta.it | M. +39. 349.4159526