Il Sole 24 ORE

La tutela dei dati di clienti, dipendenti e fornitori va adeguata entro il 25 maggio

Studi, 2mila euro per la privacy

È la spesa dei professionisti tra tecnologie e consulenze esterne

La privacy costa. Per uno studio professionale medio-piccolo la gestione e la messa in sicurezza dei dati personali di dipendenti, clienti e fornitori comporta, di media, un esborso annuo tra i 1.000 e 1.500 euro.

Spesa imputabile soprattutto alla consulenza di un esperto in grado di valutare i rischi e mettere lo studio nelle condizioni di rispettare le regole sotto il profilo della modulistica (per esempio, quella per la richiesta del consenso al trattamento dei dati) e della protezione delle informazioni.

Costi che nel prossimo futuro lieviteranno. A bilancio lo studio dovrà mettere almeno altre 500 euro l'anno, perché gli adempimenti della privacy si faranno più stringenti con l'operatività, dal 25 maggio, del regolamento europeo.

Altra spesa può essere la sottoscrizione di una polizza assicurativa contro, per esempio, atti di pirateria informatica con conseguente furto dei dati. Intanto, c'è chi sta scegliendo la soluzione di trasferire tutti i dati personali dello studio sulla "nuvola". Anche in questo caso pagando, s'intende.

Cherchi e Imperiali • pagina 7

Il Sole 24 ORE

Professionisti

COME GESTIRE LE REGOLE EUROPEE

L'esborso

Per la consulenza ora si spendono in media 1.500 euro ma con gli obblighi Ue saliranno

Le soluzioni

C'è chi opta per il fai-da-te e chi si affida a pacchetti pronti e coperture assicurative

Effetto privacy negli studi: costa di più tutelare i dati

Il debutto a maggio delle nuove norme pesa sui «piccoli»

Antonello Cherchi

Dai mille ai 1.500 euro l'anno: questo il costo della privacy per gli studi professionali di medie e piccole dimensioni. Esborso richiesto soprattutto qundo ci si rivolge a un consulente esterno. Una spesa che peserà sempre di più sui bilanci, perché con l'operatività, a partire dal 25 maggio, del regolamento europeo, ci saranno almeno altri 500 euro l'anno da destinare alla gestione dei dati personali che transitano per gli studi professionali, a cominciare da quelli dei clienti. Aumentano, infatti, gli obblighi (si veda l'infografica).

Adempimenti mal digeriti dai professionisti, che finora hanno risposto principalmente in due modi: il fai da te, adottato in particolare negli studi legali, più versati agli aspetti giuridici della riservatezza; oppure ricorrendo a consulenze esterne, alle quali, di solito, si affida l'intero pacchetto-privacy: dalla predisposizione della modulistica alla vera e propria protezione dei dati.

Ci sono poi studi che vanno più in là e stipulano una polizza per tutelarsi contro rischi particolari, come un atto di pirateria informatica con conseguente richiesta di riscatto per la restituzione dei dati trafugati. Oppure c'è chi, per non doversi occupare in prima persona delle misure di protezione, trasferisce i dati sulla "nuvola", delegando al gestore la loro tutela. «Uno strumento - sottolinea Matteo Colombo, presidente di Asso Dpo, associazione di formazione e consulenza in materia di privacy - che sta prendendo sempre più piede. I gestori, come per esempio Google, vendono pacchetti per conformarsi al regolamento Ue trasferendo i dati sul cloud».

È in atto una corsa contro il tempo perché, anche se le nuove norme europee sulla riservatezza si conoscono da quasi due anni, è in questi mesi che si sta affrontando il problema. «Abbiamo inviato di recente - spiega Marco Cuchel, presidente dell'Associazione nazionale commercialisti - una circolare a tutti gli iscritti per ricordare i nuovi obblighi e per segnalare un kit, disponibile grazie a una convenzione, con le misure per mettersi in linea con il regolamento e fare una valutazione ponderata dei rischi».

È ancora Cuchel a spiegare i motivi dell'affanno: «La normativa sulla privacy è stata sempre vissuta dagli studi medio-piccoli come un fastidio, perché invasiva rispetto al lavoro quotidiano. È una legislazione nata per le grandi realtà e traslata senza graduazione sul resto dei professionisti».

Ora, però, la prospettiva europea (regole uguali per tutti) e il giro di vite sulle sanzioni rende tutto più urgente. «Finora l'attenzione sulla privacy da parte di molti studi professionali - afferma Antonello Bevilacqua, componente dell'Organismo congressuale forense - non è stata massima. Anche perché le regole sulla riservatezza sono state vissute male: sono state varate senza sentire le categorie e hanno rivoluzionato il nostro lavoro. Se, però, la situazione fino a oggi è stata tollerata, nel futuro non lo sarà».

Gli avvocati hanno in genere scelto il metodo fai-da-te. Il regolamento europeo, però, porta nuovi adempimenti e soprattutto un nuovo approccio: dal concetto di *accountability* a quello di *privacy by design* e *privacy by default*. Potrebbe, dunque, essere necessario rivolgersi all'esterno.

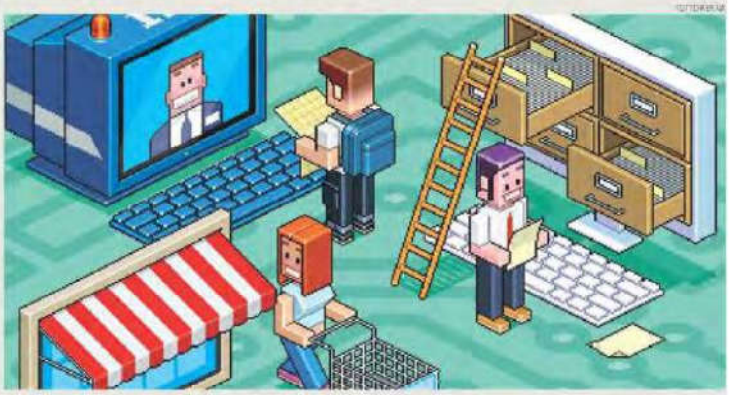
È quanto solitamente fanno gli altri professionisti. «Chiamiamo in causa un consulente - aggiunge Cuchel - con un costo che, mediamente, è di 1.500 euro l'anno. Un esborso non di poco conto nel bilancio di uno studio medio-piccolo. E ora dovremo preventivare un aggravio di circa 500 euro».

«È necessario mettersi nell'ottica che la privacy è un processo - commenta Colombo - e va affrontato secondo la cultura della *com-*

Il Sole 24 ORE

pliance, consapevoli che il costo per un corretto trattamento dei dati alla fine si trasforma in un valore aggiunto per lo studio».

Il manuale a misura di riservatezza in 14 punti



01 | NORME APPLICABILI
Oggi
Il codice della privacy (Dlgs 196/2003)
Dal 25 maggio
Il regolamento europeo 2016/679 (Gdpr, General data protection regulation, ovvero regolamento generale sulla protezione dei dati)

02 | OBBLIGO DI INFORMATIVA
Come si applica oggi
Per clienti, dipendenti, collaboratori, fornitori, ecc. l'informativa può essere anche orale, una-tantum, e fornita mediante l'affissione della stessa nei locali dello studio. L'informativa non è dovuta per la difesa in giudizio o per investigazioni difensive e se i dati non sono raccolti presso l'interessato
Come cambierà il 25 maggio
L'obbligo nella sostanza non cambia. Il regolamento europeo insiste sulla chiarezza e semplicità dell'informativa, che deve, tra l'altro, contenere il riferimento, quando è previsto, del responsabile della protezione dei dati (Dpo)

03 | CONSENSO DELL'INTERESSATO PER L'UTILIZZO DEI DATI COMUNI
Come si applica oggi
Il consenso non è necessario se i dati personali comuni sono utilizzati:
- per fini difensivi;
- per eseguire un contratto;
- per soddisfare un obbligo di legge (per esempio: antiriciclaggio);
- per dati di fonte pubblica (per esempio: dati dell'anagrafe);
- per dati economici (per esempio: codice fiscale).

Al di fuori di questi casi, per il trattamento dei dati è necessario acquisire il consenso dell'interessato
Come cambierà il 25 maggio
Le regole non cambiano ma il consenso non deve essere più documentato per iscritto

04 | CONSENSO DELL'INTERESSATO PER L'UTILIZZO DEI DATI SENSIBILI
Come si applica oggi
Il consenso non è richiesto se i dati sensibili sono trattati:
- per fini di difesa in giudizio o per investigazioni difensive, previa autorizzazione del Garante;
- analogamente per dati su condanne penali o lo stato di condannato o indagato (dati giudiziari);
- per trasferimenti esteri di dati per gli stessi motivi;
- per la gestione di rapporti di lavoro e per la sicurezza sul lavoro;
- per i dati sensibili trattati in conformità all'autorizzazione generale n. 1 del Garante;
- per i dati giudiziari trattati in conformità all'autorizzazione generale n. 7 del Garante.

Al di fuori di questi casi, per il trattamento dei dati è necessario acquisire il consenso dell'interessato
Come cambierà il 25 maggio
Le condizioni non cambiano, ma le autorizzazioni del Garante potranno essere rivisitate

05 | NOTIFICAZIONE AL GARANTE
Come si applica oggi
La notificazione va effettuata solo in casi particolari. Sono esonerati dall'obbligo i trattamenti dei dati personali finalizzati a investigazioni difensive o alla difesa in giudizio
Come cambierà il 25 maggio
Non è più prevista

06 | FAR VALERE I PROPRI DIRITTI
Come si applica oggi
L'interessato ha il diritto di sapere se ci sono dati che lo riguardano; se esistono, gli devono essere comunicati in forma intelligibile. Può chiedere che i dati siano aggiornati o integrati e, se sono trattati illegittimamente, che vengano cancellati o resi anonimi.
Il diritto è sospeso se pregiudica le investigazioni difensive o il diritto di difesa
Come cambierà il 25 maggio
Le regole non cambiano, con qualche diritto in più, come la restrizione d'uso pendente una contestazione

07 | REGISTRO DEI TRATTAMENTI
Come si applica oggi
Non è più dovuto dopo l'abolizione del Dps (documento programmatico della sicurezza)
Come cambierà il 25 maggio
Il regolamento introduce l'obbligo per le organizzazioni con più di 250 dipendenti, ma l'adempimento vale anche per quelle organizzazioni al di sotto di tale tetto se il trattamento include dati sensibili o giudiziari

08 | PRIVACY BY DESIGN E BY DEFAULT
Come si applicano oggi
Non previste
Come cambierà il 25 maggio
Il titolare e il responsabile del trattamento – dopo aver valutato il contesto, le finalità del trattamento, le soluzioni tecnologiche a disposizione e i costi – devono adottare misure per prevenire i rischi sulla privacy (privacy by design). Inoltre, devono fare in modo che vengano utilizzati, per impostazione predefinita, solo i dati necessari per ogni specifico trattamento (privacy by default)

09 | VALUTAZIONE D'IMPATTO DELLA PROTEZIONE DEI DATI
Come si applica oggi
Non prevista
Come cambierà il 25 maggio
Da attuare quando il trattamento presenta rischi potenzialmente elevati per gli interessati

10 | ACCOUNTABILITY
Come si applica oggi
Non prevista
Come cambierà il 25 maggio
Principio per cui il titolare – una volta valutato l'ambito, le finalità dell'uso dei dati personali e i rischi connessi – adotta una serie di misure organizzative e tecniche che prevengano i problemi e lo mettano nelle condizioni di dimostrare l'adeguamento al regolamento Ue

11 | SICUREZZA DEI DATI
Come si applica oggi
Misure minime e adeguate da adottare
Come cambierà il 25 maggio
Approccio basato sul rischio

12 | OBBLIGHI DI PROTEZIONE DEI DATI NEL RAPPORTO CON I CLIENTI
Come si applica oggi
Definiti con la lettera di incarico
Come cambierà il 25 maggio
L'obbligo non cambia

13 | DATA BREACH
Come si applica oggi
Non previsto
Come cambierà il 25 maggio
Nel caso di violazione dei dati (per esempio, per un attacco informatico) il titolare lo deve comunicare al Garante entro 72 ore. Lo deve comunicare anche agli interessati, se il rischio è alto e a meno che non dimostri di aver adottato misure di sicurezza adeguate

14 | SANZIONI
Come si applicano oggi
Previste sanzioni amministrative e penali: per le prime non si va oltre i 300 mila euro
Come cambierà il 25 maggio
Vengono inasprite le sanzioni amministrative pecuniarie, che possono - tenuto conto dei principi di proporzionalità - arrivare a 20 milioni di euro

Il Sole 24 ORE

IL GLOSSARIO

Accountability
■ Principio di "responsabilizzazione", cioè ogni azienda deve essere in grado di dimostrare la propria conformità al Gdpr

Dpia
■ Data protection impact assessment o valutazione d'impatto sulla protezione dei dati: consiste nella valutazione dei rischi derivanti dal trattamento di dati personali per i diritti e le libertà degli interessati nonché delle misure atte a mitigarli; obbligatoria quando si presume un rischio elevato

Dpo
■ Data protection officer (responsabile della protezione dei dati) nuovo organo indipendente di sorveglianza circa l'effettività del sistema realizzato dall'azienda per essere conforme al Gdpr; obbligatorio nei casi previsti dalla legge

Data breach
■ Qualsiasi violazione di sicurezza riguardante dati personali, come la distruzione, l'accesso, la modifica o la divulgazione non autorizzati dei dati, oppure la perdita degli stessi

Dato personale
■ Qualsiasi informazione suscettibile di identificare un individuo

Gdpr
■ General data protection regulation ovvero il regolamento dell'Unione europea 2016/679 del 27 aprile 2016. Il regolamento diventerà operativo il 25 maggio prossimo in tutti i Paesi Ue , dopo due anni durante i quali è stato dato modo agli operatori di adeguarsi alle nuove regole. Il regolamento, che non ha bisogno di recepimento, manda in soffitta la direttiva 95/46/Ce, dalla quale hanno preso spunto le varie normative nazionali sulla privacy ora in vigore, compreso il codice italiano (il Dlgs 196/2003)

Privacy by default
■ La protezione dei dati personali deve risultare come impostazione predefinita: vanno utilizzati solo i dati personali necessari allo specifico scopo legittimo perseguito e unicamente per il tempo essenziale allo scopo

Privacy by design
■ Il profilo della protezione dei dati personali deve essere affrontato sin dalla fase di concepimento di nuovi progetti o processi, prodotti o servizi

Registro dei trattamenti
■ L'elencazione sistematica di tutti i trattamenti dei dati personali effettuati dall'azienda con indicazione dei principali elementi di dettaglio atti a identificarli

Titolare del trattamento
■ L'azienda o l'ente pubblico che ha potere decisionale sull'uso dei dati personali di propria pertinenza