CIRCOLARE N. 36 DEL 04 GIUGNO 2018

PRIVACY: LIVELLO DI SICUREZZA ADEGUATO AL LIVELLO DI RISCHIO

Rif. normativi e di prassi: *Regolamento 679/UE/2016*

In sintesi

Anche i soggetti che esercitano un'attività professionale, sono tenuti, ai fini dell'applicazione del Regolamento Ue 679/2016 (GDPR), a porre particolare attenzione al sistema di sicurezza e protezione dei dati dei propri clienti.

Il professionista, infatti, ai sensi dell'art. 24 par. 1 del Regolamento Ue 679/2016 (GDPR), è obbligato a mettere in atto – nonché riesaminare ed aggiornare – misure tecniche e organizzative adeguate volte a "garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento". Tale disposizione è l'espressione del principio generale di responsabilizzazione ("***accountability***"), che, rispetto al Codice della privacy, affida allo stesso titolare del trattamento (e al responsabile) il compito di valutare in maniera autonoma, fra l'altro, nell'ambito dei principi generali di integrità e riservatezza applicabili al trattamento, l'adeguatezza della "sicurezza" dei dati personali contro il rischio, ad esempio, di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentali (art. 5, par. 1, lett. f) e par. 2 del Regolamento).

Come precisato nel considerando n. 78 del Regolamento, il titolare a fini probatori dovrebbe adottare politiche interne e attuare misure che soddisfino, in particolare, i principi della protezione dei dati fin dalla progettazione, cioè prima di procedere al trattamento stesso dei dati, e per impostazione predefinita (sono i c.d. principi della "***privacy by design***" e "privacy by default").

L'approccio concettuale è completamente innovativo, in quanto impone al professionista l'obbligo di impostare un vero e proprio "progetto" relativo agli strumenti di tutela dei dati personali (art. 25 del Regolamento). Le misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, offrire trasparenza circa funzioni e trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati.

Rispetto al Codice della privacy (art. 33 e allegato B), non sono, quindi, più previste misure minime di sicurezza, ma è il titolare del trattamento (e il responsabile) a dover garantire un "livello di sicurezza adeguato al rischio", tenuto conto di una serie di elementi, quali, fra

l'altro, stato dell'arte, costi di attuazione, finalità del trattamento, probabilità e gravità dello stesso rischio per i diritti e le libertà delle persone fisiche (art. 32 par. 1 del Regolamento).

Ciò vuol dire che l'adozione delle misure di sicurezza deve passare prima attraverso un **processo valutativo e una specifica mappatura dei rischi di trattamento**, che andrà contestualizzata, caso per caso, rispetto alle singole organizzazioni.

Con un rischio elevato valutazione di impatto

Qualora un tipo di trattamento presenti, poi, un rischio "elevato" per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35 del Regolamento – DPIA).

Dal punto di vista più operativo, alcuni esempi di misure di sicurezza sono stati forniti dal CNDCEC e dalla FNC con il documento di aprile 2018.

Per gli archivi cartacei, viene, nel dettaglio, richiamato l'utilizzo di un armadio chiuso a chiave, con la previsione delle opportune modalità per l'accesso solo ai soggetti autorizzati al trattamento nei casi e per le finalità previsti, a titolo esemplificativo a collaboratori e tirocinanti.

In tale ambito, vi è la previsione anche di dispositivi anti intrusione, allarmi, porte blindate.

Quanto ai sistemi informatici, si fa riferimento all'uso di adeguati software di protezione, quali antivirus e firewall; occorrerebbe, poi, prestare attenzione all'aggiornamento periodico delle password per l'accesso alla rete, al monitoraggio degli accessi e a salvataggi periodici e programmati dei dati trattati elettronicamente.

L'adozione di tali misure è volta a prevenire violazioni, sia pur accidentali, dei dati trattati, che, se non affrontate in modo adeguato e tempestivo, possono provocare danni fisici, materiali o immateriali alle persone fisiche, come nel caso, per i professionisti, della perdita di riservatezza dei dati personali protetti da segreto professionale (considerando n. 85 e artt. 33 e 34 e del Regolamento).

Una descrizione generale delle misure di sicurezza è prevista anche nel nuovo registro delle attività di trattamento, la cui tenuta è posta a carico del titolare e del responsabile del trattamento; la sua predisposizione costituisce uno strumento utile ed "opportuno" – al di là dei casi specifici di obbligatorietà – per dimostrare la conformità al regolamento (art. 30 e considerando 82 del Regolamento). Infatti, come precisato dal Garante della privacy nella

Guida all'applicazione del regolamento europeo, il registro rappresenta "parte integrante di un sistema di corretta gestione dei dati personali"

Si ricorda alla gentile clientela di aggiornare tutte le informative privacy necessarie in conformità a quanto disposto dal Regolamento UE, ivi comprese le fatture emesse ai clienti che dovranno riportare frasi quali:

"Ai sensi del D.Lgs. n.196/2003 e del Regolamento 679/UE/2016 Vi informiamo che i dati di Vostra pertinenza saranno utilizzati per gli adempimenti di legge, per la gestione amministrativa del rapporto e per l'adempimento degli obblighi contrattuali".