GDPR

(General Data Protection Regulation)

Che cosa comporta per te e la tua azienda la nuova regolamentazione europea per la protezione dei dati?

L'Unione Europea (UE) ha modificato le norme sulla protezione dei dati. Le modifiche sono ora legge ed entreranno in vigore in tutta l'UE il 25 maggio 2018. Le nuove norme sono denominate Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation) e si applicano a tutti, dalle autorità pubbliche alle piccole e medie imprese. Tali modifiche influenzeranno il modo in cui operiamo nel nostro business.

Cos'è la protezione dei dati dell'UE?

Nell'UE sono in vigore norme giuridiche per la raccolta e il trattamento dei dati personali. Chiunque raccolga o tratti dati personali deve **proteggerli da qualsivoglia uso improprio e rispettare una serie di disposizioni legislative.** Il GDPR aggiorna le norme oggi in vigore.

Queste nuove norme si applicano ai dati detenuti in forma elettronica e cartacea?

Sì. Il GDPR si applicherà ai **dati detenuti in forma sia elettronica (come e-mail e database) che cartacea (con poche eccezioni).** Ciò significa che siamo responsabili anche degli archivi cartacei: **dobbiamo conservarli in modo sicuro e distruggerli in sicurezza (ad esempio utilizzando un distruggidocumenti sicuro)** quando non sono più necessari.

In quali tipi di sanzioni può incorrere un'azienda in caso di violazione delle norme?

In base alle nuove norme in materia di protezione dei dati, le autorità competenti possono imporre sanzioni elevate in caso di violazioni. La sanzione può raggiungere i **20 milioni di euro oppure il 4% del volume d'affari globale annuo di un'azienda**, a seconda di quale importo è maggiore. Anche se non tutte le violazioni porteranno alla sanzione più elevata, vedersi comminare una sanzione, sia pure minima, non è un'opzione ammissibile: il rispetto delle norme da parte di tutti è fondamentale.

Le aziende dovranno fare di più?

Sì. In base alle nuove norme, ogni azienda avrà maggiori responsabilità e obblighi. In particolare, **alle aziende viene richiesto di adottare misure tecniche e organizzative a garanzia del trattamento corretto dei dati.** Per valutare il corretto livello di sicurezza è necessario considerare i rischi connessi al trattamento dei dati, in special modo quelli legati a una distruzione accidentale o illegale. Occorre anche essere in grado di dimostrare quali misure sono state intraprese in caso di controlli da parte delle autorità competenti. Una parte significativa, sotto questo aspetto, consiste nel controllare a chi vengono inviati i dati personali: ad esempio sarà necessario verificare anche le procedure adottate dalle aziende con cui si collabora.

Kratos

Quali sono le principali novità?

Scopri con questo simbolo degli importanti suggerimenti sul perché un **distruggidocumenti** può esserti utile

1

Sanzioni: sono ora particolarmente aspre, in quanto si può arrivare ad una multa **fino a 20 milioni di Euro o fino al 4% del fatturato globale annuo**. Viene preso come riferimento il **fatturato mondiale;** quindi i gruppi internazionali rischiano di vedersi colpiti dalla sanzione anche in caso essa vada a punire una sola filiale o consociata in un unico paese. Inoltre non è più ammesso il pagamento anticipato in forma ridotta.

Il **Garante della Privacy** resta l'autorità competente sia per comminare le sanzioni, sia per effettuare i controlli (tramite la Guardia di Finanza o le altre forze di Polizia).

Un **distruggidocumenti** nella propria dotazione di strumenti per la protezione dei dati può essere una buona carta a proprio favore durante i controlli; ci sono stati in passato molti casi in cui l'autorità che ha effettuato l'ispezione ne ha richiesto la presenza

2

Principio di responsabilità: il titolare ed il responsabile del trattamento dei dati sono tenuti a dimostrare di aver adottato **misure di sicurezza adeguate** e sempre aggiornate. I dati vanno **mappati periodicamente, gestiti, protetti nel modo più adeguato** (il precedente ordinamento parlava di «misure minime di sicurezza») e distrutti quando non servono più, e l'onere di dimostrare di aver fatto tutto il possibile ricade sempre sul titolare del trattamento.

Tra le **misure di sicurezza adeguate** rientra sicuramente la presenza di un distruggidocumenti, essenziale per eliminare in modo sicuro i dati non elettronici che hanno esaurito la loro ragione di essere in azienda

3

Privacy by design e by default: la protezione dei dati deve essere considerata **fin dal momento in cui si progetta una procedura aziendale che coinvolga dati di terzi;** non sarà più ammissibile detenere dati che non servono alla specifica operazione per cui sono richiesti.

Fin dal momento della **progettazione delle procedure aziendali** che coinvolgono il trattamento di dati, è opportuno considerare l'acquisto di un distruggidocumenti pronto all'uso in caso di necessità!

4

Diritto all'oblio: se ne parlava da anni, per la prima volta viene formalizzato in legge il diritto dell'interessato a richiedere la cancellazione o la distruzione di tutti i dati che lo riguardano. Il responsabile del trattamento deve rispondere con celerità (non oltre 3 mesi dalla richiesta).

Il **diritto all'oblio** riguarda anche i dati detenuti in forma cartacea, che vanno distrutti celermente in caso di richiesta da parte dell'interessato

Dove posso trovare maggiori informazioni?

Le nuove norme sono disponibili qui sul sito Web della Commissione europea. **http://ec.europa.eu/justice/data-protection/**.

Fellowes WORK BETTER™

Kratos