

## IL REGOLAMENTO EUROPEO IN PILLOLE: LE NOVITA' D'IMPATTO PER LE AZIENDE

L'ENTRATA IN VIGORE E' STATA LO SCORSO 25 MAGGIO 2016 E LA SUA APPLICAZIONE E' PREVISTA PER IL 24 MAGGIO 2018.

**ACCOUNTABILITY:** e' il principio dominante della normativa. l'azienda dovra' essere sempre in grado di dimostrare la compliance al regolamento attraverso forme di garanzia ex ante.

La responsabilizzazione dell'azienda e' totale e pro attiva.

Occorrerà non solo l'adozione di misure tecniche ma, soprattutto la predisposizione di policy interne che garantiscano il rispetto delle norme da parte del personale dipendente.

**DATA BREACH:** le aziende dovranno notificare all'autorità garante le violazioni entro 72 ore e, nei casi più gravi, informare gli interessati al trattamento coinvolti dalla violazione.

**DIRITTI DEGLI INTERESSATI:** sono stati potenziati (diritto all'oblio, limitazioni del trattamento ecc.) sarà necessario prestare la massima attenzione alle richieste provenienti da qualsiasi fonte, in particolare, occorrerà istruire i propri dipendenti a riconoscere le forme di esercizio dei diritti da parte degli interessati.

**REINTRODUZIONE DELL'OBBLIGO DI ISTRUIRE/FORMARE LE PERSONE** addette al trattamento dei dati artt. 29 e 32

**SICUREZZA DEL TRATTAMENTO:** tutte le aziende dovranno effettuare un'analisi dei rischi incombenti sui dati al fine di porre in essere le misure tecniche e organizzative (policy) adeguate per abbassare il livello di rischio rilevato.

**VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI:** è richiesta una specifica analisi ex ante sui trattamenti indicati nell'art. 35.

**SANZIONI FINO A 20.000.000 DI EURO O PER LE IMPRESE FINO AL 4% DEL FATTURATO MONDIALE:** per la prima volta sono previste anche per la violazione dei principi di base del trattamento quali liceità, correttezza, trasparenza, finalità dichiarate, adeguatezza, pertinenza, condizioni per il consenso e trattamento di dati sensibili .

LE AZIENDE HANNO 2 ANNI DI TEMPO PER UNIFORMARSI E OCCORRE ESSERE PRONTI SIN DA SUBITO. LE AUTORITA' GARANTI STANNO GIA' LAVORANDO ASSIDUAMENTE E CHIEDONO COLLABORAZIONE ATTRAVERSO IL RAGGIUNGIMENTO DA PARTE DI TUTTE LE IMPRESE DELLA CONFORMITA' ALL'ATTUALE DECRETO 196/03 DA CONSIDERARSI BASE DI PARTENZA PIU' CHE SOLIDA PER AFFRONTARE LE NOVITA'.

E A PROPOSITO DI CONFORMITA' DI SEGUITO UN BREVE ELENCO DEGLI ADEMPIMENTI AI QUALI E' INDISPENSABILE AVERE ADEMPIUTO:

**SITO WEB:** deve essere a norma, ogni form di raccolta dati deve avere un'informativa specifica con le richieste di consenso esatte. Anche i dati di navigazione devono avere l'informativa (informativa sito). Occorre una gestione dei cookie in linea con quanto enunciato dal Garante nel provvedimento 8 maggio 2014. Il Garante privacy quasi ogni giorno emana sanzioni sui siti.

**INFORMATIVE:** è importante capire che il contenuto obbligatorio declinato all'art. 13 è imprescindibile, ma è altrettanto importante sapere quali informative sono da utilizzare e come farlo.

L'evolversi della normativa ha consentito di semplificare la metodologia di comunicazione con l'interessato.

**CONTROLLI - ART. 4 STATUTO DEI LAVORATORI** (riformato dal Job Act) -: prevede che per effettuare controlli sugli strumenti di lavoro, il lavoratore deve essere preventivamente informato e istruito sulle modalità di svolgimento degli stessi e sulle conseguenze. Per essere conformi è necessario adottare policy in linea con il Codice Privacy come espressamente previsto dall'art. 4.

**MARKETING, VIDEOSORVEGLIANZA, GEOLOCALIZZAZIONE, BIOMETRIA, CLOUD:** prevedono vari adempimenti specifici (notifiche, nomine....) indicati nei provvedimenti del Garante dedicati all'argomento.

**MISURE DI SICUREZZA:** quanto previsto dall'all. B e da successivi provvedimenti (amministratore di sistema, internet e posta elettronica ecc) deve essere assolutamente conseguito. La sicurezza dei dati è il primo punto da rispettare per l'attuale normativa e per il Regolamento europeo. Non solo sicurezza informatica dei dati ma anche dei trattamenti raggiungibile attraverso policy e formazione.

**NOMINE AGLI INCARICATI:** il Garante, attraverso la Guardia di Finanza, ha spesso elevato sanzioni per la mancata adozione di nomine specifiche agli incaricati.

**TRATTAMENTO DI DATI IN ESTERNO:** l'attuale normativa e ancor più quella europea obbligano a regolare i rapporti con i soggetti ai quali affidiamo trattamenti di dati. Il Regolamento impone la nomina a responsabili esterni.

PER VERIFICARE SE GLI ADEMPIMENTI SONO STATI ADEMPIUTI SI CONSIGLIA UN AUDIT ACCURATO IN LINEA CON QUANTO PREVISTO DALLA ISO 19011 E DAI PROVVEDIMENTI E LINEE GUIDA DEL GARANTE..