GDPR REV. 1

COS'E' IL GDPR

Il **GDPR**, acronimo di **General Data Protection Regulation**, è il **nuovo Regolamento UE** (2016/679) **per la protezione dei dati personali dei cittadini europei**. Sostituisce la Direttiva 95/46/EC (tutela delle persone fisiche con riguardo al trattamento dei dati personali e privacy) ed **entra in vigore il 25 Maggio 2018**. Il GDPR si pone come obiettivo quello di regolamentare come le aziende elaborano, memorizzano e distruggono i dati personali degli utenti e semplifica il contesto normativo che riguarda gli affari internazionali, unificando e rendendo omogenea la normativa privacy dentro l'UE.

COS'È UN DATO PERSONALE

Sono **dati personali** le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc. Sono classificabili in tre categorie:

- **dati identificativi** cioè quelli che permettono l'identificazione diretta, come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc.
- **dati sensibili** cioè quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale
- **dati giudiziari** cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato

NOVITÀ PIÙ IMPORTANTI INTRODOTTE DAL GDPR

- **Obbligo di notifica** (entro 72 ore) all'autorità vigilante nazionale e agli utenti interessati in caso di eventuali fughe o compromissioni di dati
- Dimostrazione con prove documentali della **piena conformità al regolamento**
- **Nomina obbligatoria del Data ProtectionOfficer** (DPO) in amministrazioni ed enti pubblici, in imprese con oltre 250 dipendenti, in caso di trattamenti su larga scala o "monitoraggio regolare e sistematico degli interessati"
- **Obbligo di trattamento dei dati** secondo una progettazione "**by design**" (lungo tutto il ciclo di vita) e "**by default**" (trattamento dati personali nella misura necessaria e sufficiente per le finalità previste)

SANZIONI PREVISTE

Per le aziende che violeranno anche solo uno degli obblighi formalizzati dal GDPR sono previstepesanti sanzioni amministrative: **fino a 20 milioni di euro**, per le imprese, **fino al 4% del fatturato totale annuo**. Anche soggetti non appartenenti agli Stati Membri, con interessi sul territorio UE o che trattino dati di cittadini UE, dovranno garantire le medesime garanzie di tutela previste dal Regolamento.

INTERVENTI PER ADEGUAMENTO AL GDPR

GESTIONE DELLA RACCOLTA, CLASSIFICAZIONE E MODALITÀ DI ELABORAZIONE DEL DATO

Per la conformità al GDPR è necessario implementare processi e tecnologie che consentano di:

a) **gestire le identità e i diritti di accesso al dato**, associando le identità digitali alle persone fisiche ed associando loro privilegi e diritti per un efficace controllo di accesso ai dati

b) **reingegnerizzare e modernizzare le applicazioni preposte alla raccolta dei dati personali**, ovvero garantire al soggetto il rispetto dei diritti di accesso, rettifica, cancellazione ed oblio, restrizione sul trattamento

c) **tracciare, catalogare e classificare i dati gestiti** per permetterne l'elaborazione controllata

ASSICURARE LA PROTEZIONE DEL DATO

Si intende la capacità di impedire la perdita o il furto di dati personali a seguito sia di intrusioni sia dall'esterno che dall'interno della propria rete. Per questo il GDPR prevede la **criptazione** come misura minima obbligatoria (misura minima = necessaria ma non sufficiente). Ma il principio va esteso anche a tutti i dispositivi (pc, tablet, portatili ma anche dischi esterni, chiavette ecc.) che vengono utilizzati per la memorizzazione di dati personali. In caso di **violazione di dati**, l'azienda deve reagire attraverso strumenti appropriati al fine di prevenire e impedire la perdita dei dati.

GESTIONE DEI DIRITTI DEL CITTADINO

Secondo il GDPR è necessario **gestire i diritti dei soggetti detentori dei dati personali**, fra cui si citano:

- il **diritto di accesso** ai dati ed alle informazioni circa il loro utilizzo e diritto alla portabilità del dato ad altro fornitore (art.15)
- il **diritto alla rettifica** di dati non corretti (art.16)
- il **diritto all'oblio**, ovvero cancellazione e ritiro dei consensi (art.17)
- il **diritto alla restrizione dell'utilizzo** (art.18)

È necessario pertanto censire tutti i vari form presenti nel portafoglio applicativo deputati alla richiesta di informazioni personali e rivederli in termini di:

a) informative sui diritti
b) richieste esplicite di consensi
c) criteri di gestione in sicurezza del dato acquisito

SICUREZZA PERIMETRALE, INTERNA ED IN MOBILITÀ

Il corretto approccio alla sicurezza sulla rete e sugli endpoint è fondamentale per garantire da una parte l'abbattimento del rischio di violazione dati e dall'altra la capacità di controllo proattivo e di reazione immediata a seguito di una violazione o di situazioni di alto rischio di violazione. È necessaria la **sicurezza perimetrale**, ovvero è opportuno tener sotto controllo il traffico in ingresso/uscita dalla rete mediante tecniche di deepanalysis. A questo va affiancato un servizio specializzato di **firewall anti-spam / anti-virus per il traffico di posta**, sia in entrata che in uscita. L'insieme rappresenta un adeguato livello di filtraggio per attacchi dall'esterno o per bloccare tentativi di attacco che partano dalla nostra rete.

VERIFICA DELLA CONFORMITÀ PER SERVIZI ESTERNALIZZATI IN CLOUD

Il ricorso molto spesso indiscriminato a **servizi in cloud** ha sovente determinato una situazione di completa perdita di controllo sugli elementi di conformità al GDPR. È pertanto necessaria una valutazione della situazione in essere all'interno dell'organizzazione al fine di:

a) individuare i servizi in cloud di storage e sharing di contenuti e verificare per quali di essi il fornitore possa contrattualmente assicurare la conformità al GDPR

b) impedire l'utilizzo di tutti gli altri servizi (mail e storage/sharing) o implementare exit strategy per ricondurre la gestione del dato sotto controllo