GDPR e Sicurezza informatica

IL NUOVO REGOLAMENTO SULLA PROTEZIONE DEI DATI

Relatore: Patrizia Amore

22 maggio 2018

Remedios Tecnologia S.r.l.

enexus

- Agenda

1. **Regolamento Privacy UE**:
   brevi cenni sulle principali novità
2. **GDPR e Sicurezza IT:**

   Un punto di equilibrio tra la rapida evoluzione del mondo digitale e la protezione dei dati.

COSA CAMBIA?

Il regolamento prevede nuovi diritti per gli individui, impone una serie di adempimenti rigorosi alle aziende e ai professionisti e, soprattutto, introduce sanzioni!

- Per i trasgressori infatti sono previste:

A GARANZIA DEI CITTADINI

- Riconoscimento di nuovi diritti

I diritti dell'interessato sono più ampi e maggiormente tutelati.

A GARANZIA DEI CITTADINI

Informativa e necessità di consensi

Chiarezza, brevità, semplicità

- Le informazioni agli interessati, è scritto, devono essere fornite in una forma "**concisa, trasparente, intelligibile e facilmente accessibile, mediante l'uso di un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori".**

Per i titolari del trattamento

- **Dovere di documentazione:**

Sarà necessario **elaborare un sistema documentale di gestione della privacy** contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento.

Viene introdotto l'obbligo di **istituire un registro dei trattamenti dei dati** con le informazioni pertinenti e le relative responsabilità anche se pare non sia obbligatorio per organizzazioni con meno di 250 dipendenti salvo che non trattino dati sensibili (secondo la definizione del Codice della Privacy attualmente in vigore) o giudiziari.

È l'applicazione operativa del **principio di rendicontazione e responsabilità** (o di "**accountability**")

- **Dovere di formazione e informazione**

  Come emerge da più fonti, non da ultimo il **Rapporto Clusit 2017**, che delinea uno scenario da incubo in **materia di sicurezza info**rmatica, l'anello debole della filiera sono le persone. A loro, in primis, deve essere dedicata un'attività di informazione e verifica che porti un innalzamento generale del livello di attenzione e fornisca i mezzi per riconoscere i frutti avvelenati della moderna industria del **malware**.

- Privacy by design e Privacy by default

  Privacy by default:devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.

  Privacy by design:ogni nuovo trattamento di dati personali dovrà essere progettato in modo da garantire la sicurezza richiesta in base ai rischi a cui èsottoposto prima di essere implementato. Anche i sistemi informatici dovranno essere progettati secondo tale principio.

- **Data Breach**

  Il titolare del trattamento deve notificare all'autorità competente – e, in casi gravi, anche all'interessato – ogni **violazione dei dati** (*data breach*) trattati entro 72 ore dall'evento.

- **Valutazione d'impatto sulla protezione dei dati**

  Quando un trattamento presenta dei rischi elevati per i dati personali degli interessati, il responsabile del trattamento deve effettuare una **valutazione di impatto preventiva**, basata sul trattamento automatizzato, prima di iniziare il trattamento.

- **La denominazione ed i ruoli degli attori**:

  il titolare del trattamento rimane tale, ma **il responsabile del trattamento è ora responsabile in solido con il titolare per i danni derivanti da un trattamento non corretto**, l'incaricato invece rimane il soggetto che fisicamente tratta i dati.

- **Il Data Protection Officer**

  E' richiesta la designazione di una nuova figura: il **Responsabile della Protezione dei Dati** (*Data Protection Officer*) nelle Aziende Pubbliche e nelle organizzazioni che trattano dati sensibili o giudiziari su larga scala oppure nel caso in cui la tipologia di dati trattati e la loro finalità richieda il controllo degli incaricati al trattamento su larga scala.

- **Responsabilità e Sicurezza del trattamento**

  (art. 24) Il titolare del trattamento deve mettere in atto **misure tecniche ed organizzative** tali da consentirgli di dimostrare che tratta i dati personali in conformità al Regolamento

  (Art. 32) Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio.

non più misure di protezione esplicite ma libertà di scelta di un sistema di controllo sulla base dei rischi individuati

sempre l'articolo 34 prevede comunque quattro esempi di misure:

- 1) la pseudonimizzazione e la **cifratura dei dati personali**
- 2) la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la r**esilienza** dei sistemi e dei servizi di trattamento
- 3) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- 4) una procedura per testare, verificare e valutare regolarmente l'**efficacia** delle **misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

- Il regolamento è organizzato in 11 capitoli e 99 articoli, ma proprio negli articoli 24 e 32 si fa un chiaro riferimento alla sicurezza informatica.

Ma cosa si intende quando si parla di sicurezza informatica?

Con la locuzione "sicurezza informatica" si intende il complesso delle **misure tecniche** volte a garantire la **protezione hardware e software** dei sistemi informatici e di **tutti i dati** in essi contenuti, in particolare dagli accessi non autorizzati leciti o illeciti, al fine di evitare la copia, la modifica e/o la cancellazione dei dati.

In tale quadro di protezione diventa fondamentale la scelta dell'infrastruttura hw e del software gestionale per il trattamento del dato

dati dei clienti su un'infrastruttura adeguata

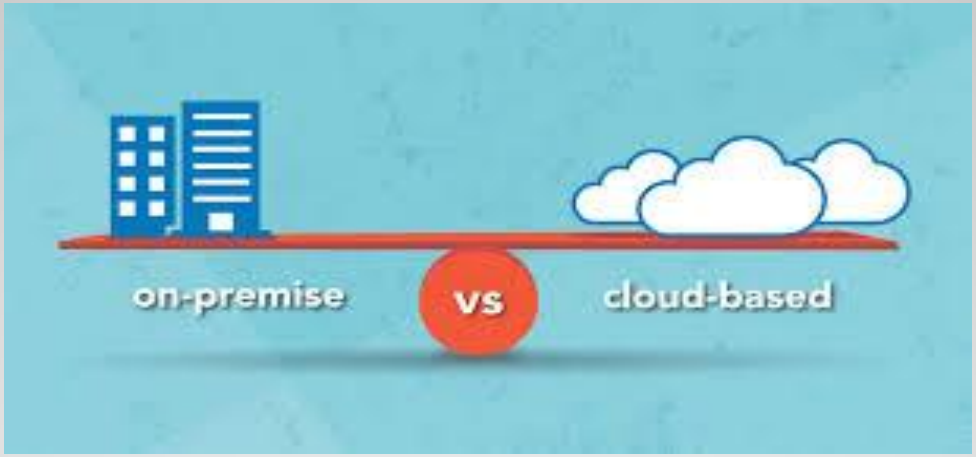
Le principali opzioni per l'installazione dei software gestionali da cui dipende quindi l'infrastruttura hw sono due: **on premises** o **in Cloud**

- **"On-Premises"** significa letteralmente "nei locali", ci stiamo riferendo al più classico dei server ospitato in una qualche stanza della vostra azienda. Quanti siano i server, se fisici o virtuali, quanti dispositivi o collegamenti ci siano non fa differenza: tutto ciò che si trova presso di voi è considerato "On-Premises".

Ecco un tipico scenario “On-Premises”:

- **“Cloud”** significa “nuvola” ed è il termine con cui oggi indichiamo un hardware oppure un software che si trova da qualche parte su Internet ed a cui accediamo da remoto. Se per noi il “Cloud” è smaterializzato, intangibile, misterioso, sappiate che dietro c’è sempre un computer acceso e ospitato in un datacenter, magari dall’altra parte del mondo. L’utente accede al server tramite la rete quindi che il server si trovi in un altra stanza o in un altro paese, da un punto di vista puramente tecnico non fa alcuna differenza.

GDPR
ON PREMISE VS CLOUD



Costo:

- **Cloud: i** costi sono significativamente più convenienti all'inizio e di solito vengono addebitati per utente. È facile prevedere i costi nel tempo e le aziende/professionisti non devono preoccuparsi di investimenti hardware aggiuntivi. Il rovescio della medaglia è che si può finire col spendere più soldi nel corso del ciclo di vita del sistema.
- **On Prem:** con soluzioni on-premises, il costo iniziale dell'investimento è più ampio, ma ammortizzato nel lungo periodo. Di contro l'utente è tenuto a pagare i costi di manutenzione hardware e personale IT in corso.

Personalizzazioni:

- **Cloud:** con le soluzioni cloud c'è meno flessibilità nelle personalizzazioni, la semplice aggiunta di una stampante nuova puo' diventare un problema. Tuttavia, ciò potrebbe significare una maggiore stabilità e aggiornamenti costanti.
- **On Prem:** le personalizzazioni sono in genere gestite direttamente dagli utenti finali con semplicità

Scalabilità

- **Cloud:** Caratteristica fondamentale e imprescindibile del Cloud Computing è quella di fornire una infrastruttura di servizi assolutamente affidabile e scalabile. È infatti possibile ad esempio a seconda delle necessità, aumentare o diminuire le risorse in uso.
- **On Prem:** Vi dà il vantaggio di una soluzione dimensionata esattamente per le vostre esigenze e completamente dedicata.

Sicurezza

- **Cloud:** fermo restando che non tutti si sentono a proprio agio nel cedere il controllo totale dei dati all'esterno quando si parla di sicurezza, molti esperti di cloud affermano che il cloud è in realtà più sicuro rispetto ai data center on-premise, perché i fornitori di questo servizio di solito si affidano a grandi team di addetti alla sicurezza e usano evoluti strumenti di sicurezza, ma è anche vero che gli enormi datacenter on cloud potrebbero essere un obiettivo più attraente per alcuni aggressori, il che aumenta il rischio.

  Fino all'attuazione del regolamento, i titolari del trattamento erano responsabili della protezione dei dati, non avevano invece responsabilità i cloud provider, a partire dal 25 maggio invece i due attori condivideranno pari responsabilità.

- **On Prem:** Si ha il controllo completo, importante per motivi di riservatezza, ma anche in questo caso è corretto ritenere che la *software house* debba essere sempre considerata responsabile del trattamento qualora oltre alla licenza vengano erogati servizi di assistenza, aggiornamento e manutenzione.

  Avere il controllo esclusivo sui dati può essere un vantaggio e risponde ad esigenze specifiche, ma è quindi sempre necessario assicurarsi che vengano applicati tutti i protocolli di sicurezza affidandosi magari esperti del settore

QUAL E' ALLORA LA MIGLIORE SOLUZIONE?

Possiamo in fin dei conti dire che dallo scontro non esce un vincitore vero e proprio ma si delinea un quadro ben preciso:

nell'ottica del GDPR sarà necessario rivolgersi sempre e solo a responsabili esperti ed accreditati con garanzie contrattuali in merito a sicurezza e difesa.

In sintesi

GDPR

Non solo la mera scrittura di documenti fini a se stessi, ma tutta una serie di interventi di adattamento che agiscono a livello di **organizzazione aziendale**, di **risorse umane**, di **gestione dei rapporti con clienti e fornitori**, oltre che di **IT**.

Possiamo ignorare il GDPR?

rischio di multe salate e danni di immagine molto ampi

Passare al GDPR

Vuol dire conoscere se stessi, conoscere la propria azienda e sapere come funziona