GDPR
le **7 domande** che vorresti fare

seeweb
THINK CLOUD

Il GDPR abbraccia vari aspetti: quelli legali, tecnologici, di processo, ed è persino relativo alle strategie di un'azienda e di un'organizzazione.
Noi di Seeweb possiamo fare la nostra parte a livello infrastrutturale.
E con questo vademecum ti diamo qualche spunto utile su come districarti senza fatica nell'ambito del nuovo regolamento.

7

Le **7 domande** che non sai a chi fare sul GDPR: perché alla fine essere compliant non è poi così complicato.

DOMANDA 1. Cos'è il GDPR?

Il GDPR o General Data Protection Regulation è un regolamento europeo (679 del 2016) che si occupa di protezione dei dati, quindi la privacy c'entra ma non è tutto.

Il nuovo regolamento, entrato in vigore il 24 maggio 2016, abrogherà la direttiva madre (direttiva 46 del 1995) **e avrà la sua piena applicabilità a partire dal 25 maggio 2018**.

Cosa importante, il GDPR coinvolge tutte le aziende che **trattano dati personali di soggetti risiedenti nell'Unione Europea** (indipendentemente dalla loro localizzazione geografica).

DOMANDA 2. C'è qualche motivo per cui mi devo dare una mossa? Ora ci sono le elezioni: figurati se stanno a pensare al GDPR!

E' un **regolamento europeo** e quindi, a differenza delle direttive (escluse quelle self-executing in quanto sufficientemente precise e dettagliate) **non necessita di alcuna azione di recepimento** (legge nazionale, decreto legislativo, ecc…) da parte del Parlamento nazionale.

Tanto per fare un esempio: nel caso il tuo server venga attaccato e tu venga derubato dei dati sensibili riguardanti tuoi clienti e questi vengano resi pubblici, qualunque giudice, a partire dal 25 maggio 2018, può condannarti, sulla base di questo regolamento europeo, a risarcire qualunque tipo di danno economico tu abbia arrecato ai tuoi clienti attraverso la "non protezione adeguata" delle informazioni che ti hanno affidato. A meno che tu non dimostri di aver messo in atto alcune misure "adeguate" di protezione dei suddetti dati.

In linea di massima, **solo chi non fa proprio nulla è pesantemente attaccabile**.

Sulle "adeguate" ci si può difendere.

Questa volta l'Europa è convinta che quella della protezione dei dati dei suoi cittadini sia cosa vitale e quindi è stata piuttosto "cattiva" con le sanzioni: fino a 20 milioni di euro e - nel caso di imprese - fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente. Inutile dettagliare i vari casi, il succo è che l'Europa vuole far capire che qua non si scherza e con queste sanzioni lo ha sancito in modo più che chiaro.

DOMANDA 3. Chi è responsabile in azienda di eventuali "mancanze" rispetto a questo regolamento?

Due sono le figure importanti:

Il **titolare del trattamento dei dati**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri (contitolari del trattamento dei dati), determina le finalità e i mezzi del trattamento di dati personali (cliente, fornitore, passante) di almeno un cittadino europeo per conto del titolare del trattamento.

Il **responsabile del trattamento dei dati**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali (cliente, fornitore, passante) di almeno un cittadino europeo per conto del titolare del trattamento. La responsabilità del trattamento dei dati non può essere affidata (Culpa in eligendo = responsabilità nella scelta del responsabile del trattamento) a figure che non presentino garanzie sufficienti a mettere in atto tutte le misure tecniche e organizzative adeguate a tutelare i diritti dell'interessato.

DOMANDA 4. Cosa devo fare per evitare di trovarmi (da titolare o responsabile del trattamento) a rispondere di eventuali danni cagionati dal trattamento?

Semplice.

Basta che tu adempia agli obblighi del suddetto regolamento e che sia in grado in ogni momento di dimostrarlo.
Obiettivo primario, dimostrare la compliance: è il principio di *accountability*. Ogni scelta presa a supporto della dimostrabilità di avere adempiuto agli obblighi imposti deve essere documentata per scritto.

DOMANDA 5. Quindi in caso di danni da cattiva protezione dei dati personali, chi paga?

Il titolare e il responsabile del trattamento dei dati **sono responsabili in solido** (cioè con il proprio patrimonio personale) **per l'intero ammontare del danno**, al fine di garantire il risarcimento effettivo dell'interessato (salvo che non si riesca a dimostrare che l'evento dannoso non gli è in alcun modo imputabile). Quindi non c'è SRL, SPA o SAPA che tenga. Niente autonomia patrimoniale perfetta in questo caso. Si è responsabili in solido di qualunque danno arrecato alla figura (cliente, fornitore o passante… europeo) di cui non abbiamo saputo proteggere i dati.

Attenzione, che potrebbe piovere sul bagnato. Nel caso in cui un giudice ti condanni a risarcire dei danni, possono poi scattare (d'ufficio?) da parte delle amministrazioni di controllo e di conseguenza le tanto temute e terribili sanzioni suddette (20 milioni / 4% del fatturato).

DOMANDA 6. Quali sono in linea generale i principi su cui mi devo basare per il trattamento e la conseguente protezione dei dati?

a] Il trattamento dei dati deve essere **corretto**, **lecito** e **trasparente**.

b] I dati devono essere raccolti per **scopi determinati**, **legittimi ed espliciti**, e trattati in modo non incompatibile con tali scopi. Non è quindi possibile detenere dati se non c'è giustificabile motivo.

c] I dati devono essere **ridotti al minimo** e quindi pertinenti e limitati a quanto necessario.

d] dati devono essere **esatti**, **aggiornati e tempestivamente cancellati** quando non più necessari.

e] E' necessario **garantire adeguata sicurezza dei dati personali**, compresa la protezione mediante misure tecniche e organizzative adeguate, dalla perdita, dal danno o dalla pubblicazione accidentale nonché da trattamenti illeciti o non autorizzati.

Il titolare del trattamento (o chi da lui delegato) deve possedere ed essere in grado di dimostrare tutte le competenze necessarie a garantire il rispetto dei principi appena elencati. Mai come in questo caso la legge non ammette ignoranza. Forse è giunto il momento di affidare i server a chi fa questo per mestiere piuttosto che tenerli in casa.

DOMANDA 7. Cosa sono tenuto a fare per poter dimostrare di aver adempiuto?

Il regolamento non fornisce una linea guida dettagliata delle misure da mettere in campo in quanto, come ben sa chi opera nel settore del trattamento - ormai elettronico - dei dati, non esiste ad oggi una ricetta perfetta capace di scongiurare attacchi esterni da parte di hacker o danni da errori accidentali. La cosa più importante è poter dimostrare attraverso una serie di azioni che ci si è presi cura del problema nel "migliore" dei modi possibile, compatibilmente al contesto.

Attualmente, alla luce della lettura del regolamento, sembra seriamente **sanzionabile l'inattività** (non fare nulla) e la **palese negligenza**.
Per fare qualche esempio:

a] Non potrai mai dire che i tuoi dati erano al sicuro da attacchi esterni se non hai previsto delle prove di intrusione condotte da soggetti esterni volte a valutare la vulnerabilità dei tuoi sistemi.
E' chiaro che nessuno è invulnerabile, ma bisogna per lo meno poter dimostrare che si sono fatte delle prove e messe in atto delle misure migliorative se necessarie.

b] Non potrai mai giustificarti davanti a un danno da perdita di dati di proprietà altrui se non hai messo in atto procedure di backup, testate con restore periodici e almeno affrontato un'analisi di disaster recovery.

c] Non potrai mai difenderti dalla perdita di dati altrui se non sarai in grado di dimostrare di aver monitorato i parametri vitali del tuo sistema (scoppio tablespace, caduta connessione, ecc…).

d] Non potrai mai giustificarti di fronte all'aver tenuto incustoditi dati cartacei riguardanti i tuoi clienti o i tuoi fornitori. Ecc…

La compliance al nuovo regolamento GDPR
è un'opportunità.

Puoi cogliere l'occasione per fare un'analisi
dei tuoi sistemi, mettere in completa sicurezza i dati
e guadagnare in termini di reputazione,
a vantaggio del tuo business.

Per info: 800112825

Seeweb srl
Via Armando Vona 66
03100, Frosinone

Via Caldera, 21 - edificio B
20153 Milano

https://www.seeweb.com
info@seeweb.com
https://www.facebook.com/seeweb.it
https://twitter.com/seeweblive

gennaio 2018

seeweb
THINK CLOUD