GDPR dallo stato dell'arte

alla miglior mitigazione

"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, [...]mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio"

(tratto dall'articolo 32 del GDPR)

Sommario

Perché questa guida

GDPR è la parola magica del momento. Basta nominare la parola GDPR e tutti entrano in fibrillazione.

Si tratta del Regolamento UE 2016/679 (General Data Protection Regulation, in breve GDPR).

Per questo motivo tutti, e dico tutti, stanno cavalcando questa ondata di attenzione verso il GDPR: chi con fini nobili, chi con fini un po' più pragmatici cercando di tirare acqua al suo mulino per vendere i propri prodotti, spesso proponendoli come la bacchetta magica che risolve tutti i problemi posti dal GDPR.

In ogni caso il regolamento che, ricordiamolo, non deve essere recepito o approvato ma è già effettivo e dal 25 maggio 2018, dovrà essere applicato universalmente.

Questa guida vuole essere un semplice vademecum ragionato e semplificato per chi si occupa di IT.

L'IT infatti ricopre un ruolo cruciale nell'allineamento al GDPR da parte delle organizzazioni.

Con questo servizio voglio aumentare la protezione dei dati trattati all'interno delle aziende clienti.

È importante, anzi necessario, che si affronti il GDPR avendo fatto proprio lo spirito per cui nasce, non vedendolo solo come un "ostacolo burocratico".

Prima di proseguire nella lettura sottolineo alcuni aspetti.

Le osservazioni che trovi nelle prossime pagine

- NON sono la medicina miracolosa
- NON sono un documento scritto e timbrato dal tuo avvocato e che puoi copiare acriticamente senza riflettere
- NON sono una sequenza di istruzioni certificate dal Garante o da qualche altro ente
- NON sono la ricetta giusta e sicura al 100% con la quale puoi mettere al sicuro tutti i tuoi clienti
- NON sono una guida valida per tutto e per tutti in quanto ogni azienda fa storia a sé e non è possibile delineare dei processi di trattamento dati che valgano universalmente per tutti
- NON sono una guida definitiva sia perché, come spiegherò più diffusamente avanti, non esistono misure di sicurezza imposte ma ognuno applicherà le proprie (secondo coscienza e competenza), sia perché, ne sono quasi certo, alcune direttive lasciano quanto meno libera interpretazione e talvolta sono addirittura impossibili da realizzare con le tecnologie di oggi all'interno dei sistemi informativi, per cui mi aspetto che arrivino direttive, sentenze, chiarimenti e ricorsi che aiuteranno tutti ad applicare meglio il regolamento: insomma non sono delle regolette, ma è una cosa che vive e si evolve.

Dopo tanti NON ecco una spiegazione più chiara di cosa sono queste pagine.

Si tratta di una guida ragionata e semplificata su quello che si può fare per proteggere i dati e il loro trattamento senza diventare paranoici, senza impedire a colleghi e clienti di lavorare per l'eccessiva imposizione di criteri di sicurezza.

È una guida positiva e propositiva. È pre-masticata e pre-digerita da un occhio informatico.

È pratica e operativa, e ti indica come e quando l'utilizzo di tecnologie e strumenti proposti, può aiutarti e mitigare i rischi e quindi aiutare ad allineare la tua aziende al GDPR.

Le chiacchiere le lascio agli altri.

Ah dimenticavo, non esiste lo strumento magico che fa tutto da solo o il programma che risolve tutte le questioni legate al GDPR. Lo spirito del GDPR è il contrario di questo.

Cosa è il GDPR e a cosa serve

Il 24 Maggio 2016 è entrato in vigore il nuovo regolamento sulla protezione dei dati, il cosiddetto GDPR.

Hai letto bene, è già in vigore, da Maggio 2016.

Ti chiedi cosa sia la data del 25 Maggio 2018 che tutti sbandierano come spauracchio per farti comprare chissà quale magico software o servizio di consulenza?

Quella è la data entro la quale è necessario allinearsi e conformarsi a questo nuovo regolamento.

Il regolamento porta innovazioni per i privati, ma anche per le aziende.

Il legislatore ha voluto dare regole chiare e uniche per tutti gli stati dell'UE. Ma il regolamento va oltre perché impone di trattare (e proteggere) i dati come si fa nella UE anche per società esterne all'UE ma che trattano dati e/o vendono beni e/o servizi a soggetti che si trovano all'interno della UE.

L'obiettivo finale di questo regolamento è accrescere la fiducia del cittadino nel consegnare i propri dati avendo la certezza che verranno trattati in maniera conforme al regolamento da tutti i paesi dell'UE.

Per le aziende cambia la visione generale del dato: si passa da obblighi e adempimenti relativi alla privacy, a una vera e propria gestione della "privacy" stessa e dei rischi che il trattamento dei dati comporta, il che significa che occorre fare un'analisi sull'impatto che il trattamento comporta e dei rischi e poi intraprendere opportune misure per mitigare questi rischi.

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability in inglese) di titolari e responsabili del trattamento, ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (artt. 23–25). Si tratta di una grande novità per la protezione dei dati in quanto viene sottolineato che è affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento stesso.

Niente più "lista della spesa" imposta e calata dall'alto circa gli strumenti minimi di protezione (ricordi il vecchio elenco di "misure minime"?), ma autonomia decisionale per ogni impresa, ente o azienda.

L'importanza del GDPR, è espressa in modo inequivocabile dall'articolo 84 che riporta l'entità delle sanzioni economiche per chi non è allineato con la normativa. Ne parlo più diffusamente nel capitolo "Se non per i dati, fallo per i soldi".

Cosa posso fare personalmente per te e la tua Azienda?

Oggigiorno il trattamento dei dati avviene quasi esclusivamente in maniera elettronica.

E se i dati sono trattati elettronicamente sarà necessario mettere in atto sistemi di autenticazione, autorizzazione, protezione, salvataggio…

Benché tu, titolare, sia responsabilizzato in prima persona dal GDPR, è anche comprensibile che il tuo lavoro sia altro di quanto appena esposto e presumibilmente è anche normale la non competenza tecnica per valutare in autonomia i possibili rischi per i dati e le possibili contromisure per mitigare tali rischi.

Sicuramente lavorando insieme possiamo andare a mettere in atto un piano affinché la tua Azienda sia **GDPR Compliant**.

Cosa cambia rispetto a prima, in sintesi

Il nuovo regolamento va a soppiantare le normative presenti nei paesi dell'Unione Europea che ogni paese aveva messo in atto dopo la direttiva europea N. 46 del 1995 sulla protezione dei dati.

Di fatto il regolamento non modifica in maniera sostanziale le norme alla base della direttiva del 1995. Al contrario amplia alcuni requisiti introducendo dei nuovi obblighi, non ultimo il principio di accountability: a titolo di esempio ti ricordi le "misure minime" presenti nell'allegato B del Decreto legislativo 196/2003?. Ecco il GDPR non impone nessun elenco specifico di misure da adottare ma sarà il titolare del trattamento a decidere come gestire e trattare i dati, a valutarne i rischi, mettendo in atto le misure per minimizzare questi rischi, e dovrà essere in grado di dimostrare di aver fatto tutto questo.

Vediamo gli **elementi di novità rispetto al passato**, in estrema sintesi

- Il ruolo attivo e proattivo dell'azienda nella figura del titolare che dovrà adottare e dimostrare di aver adottato politiche adeguate e conformi al regolamento in merito alla protezione dei dati.
- Si introduce il principio dell'applicazione del diritto della UE anche ai trattamenti svolti al di fuori della UE, se relativi a beni e/o servizi offerti nella UE o relativi al monitoraggio di cittadini all'interno della UE. (Se hai un ufficio a Singapore e vendi prodotti a soggetti interessati che stanno in Italia, allora anche se l'ufficio è a Singapore i dati dovranno essere trattati e protetti come dice il GDPR).
- Vengono introdotti i concetti di "privacy by design" e di "privacy by default". Il primo sta a indicare che prima di raccogliere e trattare i dati devi mettere in pista un processo che dall'inizio alla fine pensi alla protezione dei dati e alla tutela del diritto alla riservatezza delle persone fisiche; il secondo sta a indicare un modus operandi che preveda la "chiusura" dei sistemi informatici di trattamento dei dati e solo dopo aver valutato i rischi si posso provvedere a una graduale "apertura".
- DPO (Data Protection Officer): l'istituzione di una figura "indipendente" responsabile del "governo dei dati" e della "privacy". Obbligatorio per un'autorità pubblica, per un ente il cui fine è il monitoraggio su larga scala e sistematico degli interessati o il trattamento su larga scala di dati particolari.
- Data Protection Impact Assessment (DPIA), non obbligatorio per aziende sotto i 250 dipendenti, è il documento che descrive i flussi di dati all'interno delle aziende e i relativi rischi per i dati.
- La segnalazione dei "data breach": ossia l'obbligo generalizzato di segnalare l'avvenuta violazione, fuga o compromissione di dati.
- La necessità di individuare i rischi (informatici e non) relativamente ai dati.
- Le sanzioni (salate!) in caso di violazione del GDPR.
- Cifratura e pseudonomizzazione dei dati personali, ossia il principio per cui le informazioni di identificazione (eventualmente profilazione) non devono essere conservate in maniera tale che sia riconducibile a una ben precisa persona.
- …

Credo che la lista non sia esaustiva delle novità, ma non mi dilungo oltre.

Una possibile strategia di approccio

Se sei arrivato fino a qui leggendo tutto quanto ho scritto prima ti faccio i miei complimenti, hai una bella resistenza!

Quindi vado dritto al sodo.

Il fatto che il 25 Maggio 2018 è la scadenza ultima per allinearsi al GDPR non significa assolutamente che il nostro Decreto Legislativo 196/2003 (la "legge sulla privacy" detto in parola povere) verrà abrogato. Il che vuol dire che, fino a prova contraria, le due normative convivono. Anzi è quanto mai opportuno mantenere "aggiornate" le implementazioni e la documentazione relative alla cosiddetta privacy (lettera di incarico a chi tratta i dati, salvataggi continui e sicuri, password sicure e cambiate di frequente, ecc.), in quanto previste anche nel GDPR in un certo qual modo.

Ma non è un cambiamento solo di termini, è un cambiamento sostanziale: l'aspetto chiave non è essere in possesso dei dati, ma saperli trattare con "coscienza" e, soprattutto, proteggere.

In questi mesi ho fatto un sondaggio tra i miei clienti e le ansie che ho riscontrato si possono riepilogare nei punti sotto riportati:

- ma il diritto all'oblio?
- come faccio a rilevare i data breach?
- come faccio a cifrare tutto?
- la mia azienda non investirà in sicurezza informatica perché non ha sufficienti fondi..…

Ti ricordo ciò che ho inserito all'inizio, quale parte dell'articolo 32 inizia con:

"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."

Quindi non è che tutti sono obbligati a tutto: ogni azienda fa storia a sé, ogni titolare decide per sé, tenuto conto delle proprie peculiarità.

Alla luce di quanto sopra tu dovrai affrontare un percorso di analisi, valutazione ed eventuale implementazione di misure tecniche e/o organizzative su quello che potrebbe essere ad esempio il censimento dei soggetti coinvolti nei trattamenti, dei trattamenti stessi e dei dati trattati, elaborazione delle lettere di incarico (anche per responsabili del trattamento, amministratori di sistema, …), delle policy aziendali e delle istruzioni agli incaricati nonché del Registro dei Trattamenti, per la formazione degli incaricati, nell'elaborazione della Valutazione di Impatto, ivi compresa l'individuazione dei rischi) e soprattutto nel sigillare misure tecniche (e non) adeguate per mitigare i rischi.

E soprattutto lo stato d'opera di mia stretta pertinenza quali, a titolo di esempio, un assessment iniziale per capire come sono strutturati i sistemi informativi, quali sono i possibili problemi e le possibili falle, e quindi quali sono le misure da implementare per mitigare i rischi.

Al fine di agevolare questo lavoro di assessment e di valutazione ho pensato di mettere nero su bianco le mie riflessioni relative ai rischi generalmente presenti in azienda e alle contromisure da mettere in campo per mitigarli.

Valutazione dei rischi e misure per mitigarli

Questa guida finisce qui.
E' stata redatta e portata a tua conoscenza al fine di sensibilizzarti alla nuova normativa europea che, nonostante sia già attiva, prenderà il suo fervore il 25 maggio 2018.
Il tempo a disposizione è ormai breve e le cose da fare sono tante e spesso complesse. Quindi, qualora tu non avessi ancora preso in considerazione l'adeguamento, non starei tanto a pensarci, ma inizierei ad approfondire l'argomento.

Di seguito riporto i miei riferimenti al fine di potermi contattare per un appuntamento in merito al servizio che, come responsabile IT in altre realtà, offro ai miei clienti.

Cordiali Saluti
Gianluca Zeri

è rappresentata da
Zeri Gianluca Pierfrancesco
Via Ambrosoli, 13
50028 - Tavarnelle Val di Pesa (FI)
Tel +39.055.80.71.874
Fax +39.055.80.91.028
Mob. +39 335.56.99.832
e-mail puntozeri@puntozeri.it

Firma per accettazione incarico

_____

Data _____

Ragione Sociale Cliente

_____

è rappresentata da

Via
Cap, Loc, Prov
Tel
Fax
Mob.
e-mail

Firma per conferimento incarico

_____

Piccolo glossario

Dati personali sono “qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale”. A norma del Regolamento, ciò include anche gli identificativi online, come gli indirizzi IP e i cookie.

Trattamento è “qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione”.

Interessato (persona fisica) indica la persona fisica “che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online”.

Titolare del trattamento (organizzazione) è “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri”.

Responsabile del trattamento (fornitori di servizio) è “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento”.

Data breach (la violazione di sicurezza) è “una violazione di dati personali che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati”.

Realizzazione collaborativa con
Sig. Claudio Panerai – Achab S.p.A.
Avv. Dr.sa Chiara Magalini – Studio Dusilaw Legal&Tax