OVERLAND TANDBERG

10 CONSIGLI ESSENZIALI PER ADEGUARSI AL GDPR

GDPR

General Data Protection Regulation
Regolamento Generale sulla Protezione dei Dati

Il 25 Maggio 2016 è entrato in vigore il **GDPR** - acronimo di *General Data Protection Regulation* ovvero il **Regolamento Generale sulla Protezione dei Dati nell'Unione Europea**.

Dopo quasi due anni dalla sua approvazione, ad oggi, mancano solamente pochi giorni al **termine ultimo per mettersi in regola - il 25 maggio 2018**.

In questa breve guida, che abbiamo redatto per voi, cercheremo di illustrarvi in maniera molto semplice che cosa sia il GDPR e quali siano i passi da seguire per essere conformi a questo nuovo regolamento.

INDICE

CHE COS'È il GDPR

Il GDPR è un regolamento pubblicato sulla "Gazzetta Ufficiale" dell'Unione Europea il 4 Maggio 2016 e prevede **disposizioni che impongono alle imprese di proteggere i dati personali, la privacy e le transazioni dei cittadini residenti negli stati membri**. Il GDPR regola anche l'esportazione di dati personali al di fuori dell'UE ed è valido anche per le numerose aziende d'oltre oceano che operano in Europa o gestiscono dati relativi a cittadini europei.

In breve la nuova normativa nasce dalla preoccupazione pubblica per la privacy dei cittadini europei benchè l'Europa abbia sempre avuto regole più severe degli Stati Uniti sull'utilizzo e gestione dei dati personali dei propri cittadini.

Il GDPR sostituisce una direttiva del **1995** quando Internet non era ancora il gigantesco mondo virtuale che è oggi. Di conseguenza, **la vecchia direttiva non affrontava molti dei modi in cui i dati vengono oggi raccolti, gestiti, trasferiti e archiviati**.

Scarica qui il documento completo in PDF:
http://bit.ly/testo-GDPR

DIRITTO DI ACCESSO

Uno dei fondamentali diritti dell'interessato garantiti dal GDPR è sicuramente il **diritto di accesso** che viene disciplinato dall'art. 15 laddove viene sancito che l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, se è in corso tale trattamento, l'accesso **ai dati e alle seguenti informazioni**:

- le **finalità** del trattamento;
- le **categorie** di dati personali in questione;
- i **destinatari** o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il **periodo di conservazione** dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;
- l'esistenza del **diritto** dell'interessato **di chiedere** al titolare del trattamento la rettifica o **la cancellazione dei dati** personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre **reclamo ad un'autorità** di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro **origine**;
- l'esistenza di un processo decisionale automatizzato, compresa la **profilazione** e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le **conseguenze** previste di tale trattamento per l'interessato.

QUALI SONO I DIRITTI DEI CITTADINI EUROPEI

Con il GDPR vengono rafforzati i diritti degli individui e la protezione dei dati.

Queste novità le stiamo gradualmente toccando con mano negli ultimi tempi grazie all'adeguamento di molte piattaforme online come i social network.

Tutto questo si traduce nella **possibilità di accedere più facilmente ai nostri dati**, nel **diritto a essere informati** su come i propri dati vengono gestiti e processati, nel **diritto a trasferire i propri dati**, in formato aperto, tra diversi fornitori.

Inoltre ogni individuo che non vuole più che i propri dati vengano trattati, e questo dimostra come non ci sia motivo per conservarli, **può esigere la loro cancellazione** (diritto all'oblio).

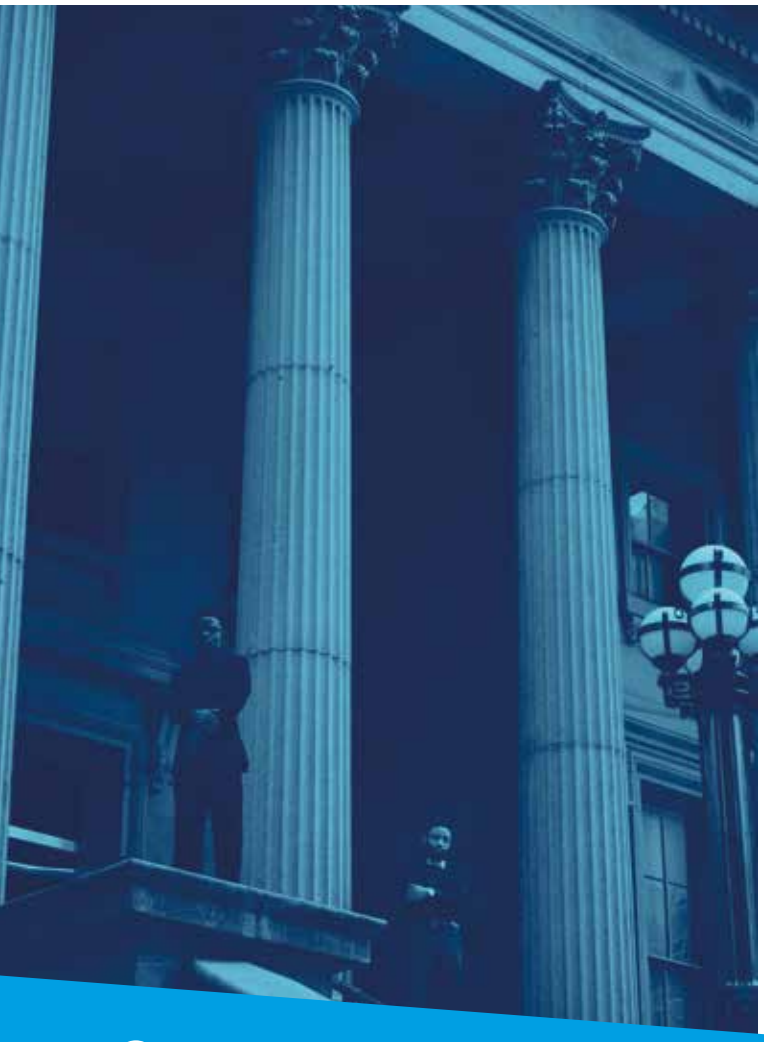
Inoltre, viene **regolamentato il trattamento dei dati del minore** (anche in relazione ai servizi di informazione offerti in forma diretta) e soprattutto, ogni individuo, acquisisce il **diritto di sapere quando i propri dati siano stati violati**.

Le imprese, le aziende, i professionisti e le organizzazioni devono notificare entro 72 ore all'Autorità Nazionale di Vigilanza (Garante Privacy in Italia) le violazioni di dati personali più gravi, cosicché gli utenti possano prendere le misure adeguate.

CHI VIGILA SUL REGOLAMENTEO E LO FA RISPETTARE

Il GDPR prevede una sola normativa e una sola autorità di vigilanza. Significa che le aziende faranno riferimento ad una singola **Autorità Europea di Vigilanza** benché non sia ancora chiaro se il ruolo del Garante della Privacy, presente in Italia, sarà soppresso o acquisirà un ruolo di controllo interno e/o di relazione con la nuova autorità garante internazionale.

Le imprese extra-UE dovranno comunque applicare la normativa europea se offriranno servizi a cittadini dell'Unione Europea.



LE SANZIONI

Il Gdpr prevede, per le non conformità, **penali fino a 20 milioni di euro** o il **4% del fatturato annuo complessivo**, a seconda di quale sia il valore più alto.

Un requisito particolarmente difficile da rispettare nella sua totalità sarà il **diritto all'oblio**. Secondo un recente sondaggio, quasi i due terzi (66%) degli intervistati, affermano di non essere sicuri di poter eliminare le informazioni personali di un individuo per sempre e questo lascia molte organizzazioni vulnerabili alle multe.

COSA BISOGNA FARE

In pratica il Regolamento applica integralmente il principio **Privacy By Design** e **By Default**, cui ogni sistema deve adeguarsi, stabilisce come **il consenso al trattamento dei dati debba essere sempre valido, esplicito e revocabile**. La salvaguardia della protezione dei dati deve essere **integrata in prodotti e servizi sin dalla fase iniziale dei processi**. Questo incoraggia alla tutela della privacy anche con l'utilizzo di pseudonimi, soprattutto nello sfruttare i benefici dei big data con minori rischi.

Il Gdpr definisce diversi ruoli per i responsabili della conformità: il **controllore dei dati** (data controller), il **responsabile del trattamento dei dati** (data processor) e il **responsabile della protezione dei dati** (DPO – Data Protection Officer). Il responsabile del trattamento definisce come vengono elaborati i dati personali e gli scopi per i quali il dato viene elaborato.

Il controllore è anche responsabile di assicurarsi che gli appaltatori esterni siano anch'essi conformi. I responsabili del trattamento dei dati possono essere gruppi interni che gestiscono e trattano i dati personali o qualsiasi società di outsourcing che svolga tutte o parte di tali attività.

Il regolamento Gdpr considera **i data processor responsabili di violazioni o di non conformità**. È possibile, quindi, che sia la società che i partner coinvolti nel processo di elaborazione, ad esempio un fornitore di servizi cloud, siano responsabili e subiscano le sanzioni, anche se l'errore riguarda esclusivamente il partner esterno.

Il Gdpr richiede al data controller e al data processor di designare un **DPO per supervisionare la strategia di sicurezza dei dati e la conformità al regolamento** e quando le aziende hanno diverse sedi o stabilimenti dovranno averne più di uno.

Le aziende devono avere un responsabile della protezione dei dati se elaborano o memorizzano grandi quantità di dati sui cittadini dell'UE, elaborano o memorizzano dati personali sensibili, controllano regolarmente le persone interessate o sono un'autorità pubblica.

IL RUOLO DEL DPO

L'art. 37 del nuovo GDPR introduce la figura del **Data Protection Officer (DPO)**, ossia il responsabile per la protezione dei dati. Si tratta di una persona fisica - potrà essere un lavoratore dipendente della società oppure un soggetto terzo esterno all'azienda - che dovrà garantire la riservatezza di tutta una serie di informazioni sensibili. Per svolgere tale attività non sarà necessaria alcuna particolare abilitazione anche perché, **al momento non esistono albi professionali o corsi di certificazione**.

Il DPO dovrà essere istituito dal titolare dell'impresa (o dal responsabile del trattamento) per assolvere a **funzioni di sostegno e verifica, consultive, formative e informative** relativamente all'applicazione del Regolamento europeo sulla privacy e fungerà da referente con il Garante per le questioni connesse al trattamento dei dati personali. La aziende obbligate ad avere il DPO saranno quelle attive proprio nel monitoraggio regolare e sistematico di dati personali o di dati relativi a condanne penali e a reati.

Lo stesso Garante, per semplificare l'identificazione, elenca una serie di esempi come: banche, assicurazioni, istituti di vigilanza, società che forniscono servizi di telecomunicazioni, gas ed elettricità, società che operano nel settore sanitario, call center, società radiotelevisive. Tra l'altro è da notare che nella lista sono compresi anche partiti politici e sindacati. Tuttavia sono esclusi alcuni enti pubblici come le forze dell'ordine.

IL RUOLO DEI RESPONSABILI DEL TRATTAMENTO DATI

La figura del DPO non corrisponde a quella dei Data Processor e per questo occorre fare chiarezza. Si parla in modo corretto di un vero e proprio **Data processor** o **Responsabile del trattamento** (Art. 28), ed **è persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento**. Spesso questa figura è rappresentata da **un fornitore delegato** per il trattamento di cui si deve verificare l'effettiva capacità di garantire la compliance GDPR.

Sono possibili infatti accordi/contratti di regolamentazione tra aziende e fornitori con questi ultimi che potrebbero trovarsi nella condizione di nominare un loro DPO. Per esempio quando ci si trova di fronte a una realtà con una vera e propria catena di trattamenti anche in un unico presidio. Accade questo quando la gestione del personale è demandata a diversi fornitori di soluzioni, anche solo in fase di processo (software per le presenze, consulenti del lavoro, successivi servizi via Web anche degli istituti di previdenza), ogni qualvolta si assista a una diramazione di fornitori esterni di soluzioni, a partire anche solo da un unico database.

I PUNTI DI ATTUAZIONE DEL GDPR PER LE AZIENDE

Riassumiamo le azioni preventive in cinque macro aree:

1. **Il pieno controllo all'accesso ai dati fisici** sia su DataBase strutturati che destrutturati:
   - Dati anagrafici e demografici;
   - Canali di comunicazione (telefono, email, codice postale);
   - ID Nazionali (codice fiscale, passaporto, targhe, tessere sanitarie);
   - Conti Finanziari e Carte di credito;
   - Identificativi digitali;
   - Riferimenti Organizzazione di appartenenza;
   - Social Media;
   - Ulteriori dati sensibili (salute, religione, indirizzo di pensiero);
2. **Identificazione dei dati personali** (accesso immediato, profilazione, deduplica e sicurezza)**;**
3. **Governo dei dati:** le policy, la governance tout court, il collegamento dei processi, gestione delle responsabilità;
4. **Strategie di protezione dei dati** (pseudonomizzazione e crittografia);
5. **Controllo rigoroso delle procedure applicate:** reportistica interna, censimenti, verifiche, gestione e rapporto con il pubblico.

IL GDPR PER LE PMI

La nuova normativa impegna e mette sotto stress anche le PMI. Affianco ai doveri esse dovrebbero ottenere anche una serie di **benefici** e di **opportunità**.

- In caso di richieste di accesso ai dati con costi in termini di tempo e risorse per le aziende, **le PMI potranno richiedere una tariffa** per fornire l'accesso e la modifica.
- Le PMI saranno **esonerate dall'obbligo di nominare un responsabile del trattamento dei dati personali nella misura in cui il trattamento dati non sia la principale attività dell'impresa**.
- Le PMI non avranno, di norma, un obbligo stringente di effettuare la **"valutazione d'impatto"**, a meno che non ci sia **un "rischio specifico"**, dato il volume di dati trattati relativi a soggetti terzi, specie in modalità elettronica.
- Le notifiche alle autorità di vigilanza sono una formalità che rappresenta un costo di 130 milioni di euro all'anno. **La riforma eliminerà definitivamente quelle ordinarie, mantenendo quelle più a rischio privacy.**

10 CONSIGLI ESSENZIALI PER ADEGUARSI AL GDPR

Il tempo ormai è poco per cui cerchiamo di fornirvi alcuni consigli per adeguarsi al GDPR nel più breve tempo possibile:

1. Elaborare una **mappa chiara**, tracciare un percorso per aggiornare i sistemi, definire le procedure di gestione. Farsi assistere da realtà che sanno bene cosa e come fare;
2. Prevedere un **piano di comunicazione per informare gli utenti** con tutte le relative procedure di avviso anche alle autorità competenti in caso di una violazione della loro privacy;
3. Disporre un **registro delle attività di trattamento** (art. 30) con strumenti di reporting aziendali allo stato dell'arte;
4. Adottare per qualsiasi processo il principio "**Privacy by Design**". Per effettuare il **Privacy Impact Assessment** sarà necessario affidarsi agli esperti che possano minimimizzare l'impatto e contenere i costi di gestione degli adempimenti;
5. **Monitorare i processi** permetterà di avere uno stato aggiornato della situazione e comprendere se modificare o mantenere la rendicontazione;
6. **Comprendere se vi rivolgete a soggetti che hanno prestato il loro consenso al trattamento**, o se potete viceversa fare a meno in quanto avete un interesse legittimo nel trattamento che non è subordinato agli interessi della persona;
7. Gli **aggiornamenti alla regolamentazione** dovranno essere apportati anche ai vostri processi quindi incaricate qualcuno a questa funzione;
8. Essere pronti a **soddisfare le richieste dei titolari dei dati** torna solo a vostro vantaggio;
9. **Trasferire i dati non è come detenerli**, approfondite anche questa tematica;
10. Adeguarsi al GDPR è **problema comune** a tutta l'UE e a tutti gli Extra-UE che trattano dati di cittadini UE.

“Siamo ormai agli sgoccioli perché mancano meno di 30 giorni alla piena efficacia del Gdpr. Pensiamo che sia ancora possibile fare qualcosa per mettersi in regola puntando sugli adempimenti essenziali ma occorre fare presto perché non c’è più tempo da perdere se non si vogliono rischiare sanzioni”.

Paolo Rossi
Italy Channel Sales Manager
Overland Tandberg

OVERLAND TANDBERG

Tandberg Data GmbH
Feldstraße 81, 44141 Dortmund, Germany
t +39 388 3459136 | s PaoloRossiIT
paolo.rossi@tandbergdata.com

sphere3d.com | overlandstorage.com | tandbergdata.com

canali social italia:
@OverlandTandberg @TandbergData_IT @tandberg-data-it

FONTI

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
http://bit.ly/EUR-lex

GDPR, le 5 cose essenziali che le aziende devono fare per adeguarsi
http://bit.ly/5essenziali-GDPR

GDPR, il DECALOGO per capire cosa bisogna fare e mettersi in regola
http://bit.ly/decalogo-GDPR

Privacy: i diritti dell’interessato nell’ottica del GDPR
http://bit.ly/diritti-GDPR