Il GDPR per le Associazioni ed Enti del Terzo Settore

Effetti dell'applicazione della normativa sulla Privacy (GDPR) per le Organizzazioni Non Profit.

IL SOFTWARE PER LA CONTABILITÀ DELLA TUA ASSOCIAZIONE

CENTRO STUDI FINANZA & PERSONA

Che cos'è il GDPR?

Il prossimo 25 maggio 2018 diventerà a tutti gli effetti applicabile il nuovo Regolamento Europeo 679/2016 (il c.d. "GDPR").

Il GDPR è un testo fortemente innovativo rispetto alla normativa vigente in materia di privacy, che si pone vari obiettivi in tema di trattamento dei dati.

I più importanti **obiettivi del GDPR** sono costituiti da:

1. delineare **principi comuni** per tutti gli Stati membri;
2. stabilire un più **alto livello di garanzie** a tutela del diritto fondamentale dei cittadini alla **propria riservatezza**.

Il GDPR ha introdotto una serie di nuovi obblighi in materia di Privacy e rafforzato quelli già previsti dalla normativa comunitaria e italiana già vigenti; esso sarà direttamente applicabile in tutti gli Stati dell'Unione, ma saranno comunque necessari ancora notevoli adeguamenti per determinati aspetti, come l'adeguamento del **sistema sanzionatorio penale** ed **amministrativo**.

La Ratio del GDPR: la tutela dei dati delle Persone fisiche

Il Regolamento ha come finalità principale e solenne "la **protezione delle persone fisiche** con riguardo **al trattamento dei loro dati personali** a tutela di un diritto fondamentale riconosciuto dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea."

Il Principio della normativa sulla Privacy

I motivi base del GDPR per poter trattare i dati possono essere riepilogati in alcuni fondamentali Pilastri. Riassumiamo di seguito questi motivi base:

- **il consenso;**
- **l'adempimento di obblighi contrattuali;**
- **gli interessi vitali della persona interessata o di terzi;**
- **gli obblighi di Legge cui è soggetto il titolare.**

Quali dati sono oggetto della Privacy?

I dati oggetto della normativa sulla Privacy possono essere suddivisi in **3 categorie**:

- i **DATI PERSONALI** rappresentati da qualsiasi informazione relativa ad una persona fisica (per esempio: il nominativo, la data di nascita o il numero di cellulare di un associato);
- i **DATI SENSIBILI** rappresentati dalle informazioni che rivelano origine razziale, etnica, opinioni politiche, convinzioni religiose, dati relativi alla salute, all'orientamento sessuale, ecc…;
- i **DATI GIUDIZIARI** che riguardano condanne penali, reati o misure di sicurezza delle persone.

ESEMPI DEI DATI OGGETTI DI PRIVACY
Dati sensibili
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 Personali
Nome
Cognome
Indirizzo
Numero di telefono
Dati Giudiziari
Anagrafe sanzioni amministrative
Carichi pendenti

Tutti questi dati sono importanti ai fini della Privacy e sono quelli ai quali si rivolge la normativa. Chi tratta dati **sensibili**, **personali** o **giudiziari** è interessato da questo nuovo adempimento.

IL CONSENSO. Trattieni i dati lecitamente?

Principio di liceità e correttezza del trattamento nei confronti dell'interessato.

Il **consenso è lecito** soltanto quando:

- ✓ l'interessato ha prestato un **consenso informato**;
- ✓ quando il trattamento è **necessario** all'**esecuzione di un contratto** di cui l'interessato è parte;
- ✓ quando il trattamento è necessario per adempiere un **obbligo legale** a cui è soggetto il titolare del trattamento;
- ✓ quando lo stesso è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- ✓ quando è necessario per l'esecuzione di un **compito di interesse pubblico** o per il perseguimento del legittimo interesse del titolare del trattamento.

Il **consenso** deve essere **prestato**:

- in modo chiaramente **distinguibile**;
- in forma facilmente **comprensibile**;
- in modo facilmente **accessibile**.

Il consenso può essere **revocato in qualsiasi momento** con la stessa semplicità con cui è stato concesso.

Privacy dei Minorenni

L'acquisizione dei dati sensibili richiede un **consenso esplicito** da parte dell'interessato. Nel caso di **minori** il consenso è valido **a partire dai 16 anni**, prima di tale età occorre raccogliere il consenso dei genitori.

Individuata la natura dei dati acquisiti dall'associazione bisogna assicurarsi che essi siano raccolti e trattati nel rispetto di precise e determinate finalità, che vanno comunicate all'interessato e poi rispettate.

Nel caso degli enti no-profit, le finalità del trattamento dei dati coincidono generalmente negli scopi istituzionali indicati nello statuto; nel caso in cui vengano impiegati per scopi ulteriori sarà necessaria un'autorizzazione specifica.

In sintesi, il percorso da seguire per conformarsi al GDPR presuppone, come passo iniziale, una mappatura delle banche dati in uso all'interno di ciascuna organizzazione non profit, volta ad individuare le caratteristiche intrinseche dei trattamenti posti in essere, in termini di dati personali raccolti, siano essi personali o sensibili, finalità perseguite, soggetti coinvolti e misure di sicurezza applicate.

INFORMATIVA Quali sono i diritti degli interessati?

L'informativa Privacy
L'interessato ha sempre diritto di conoscere, attraverso un'informativa, ovvero un documento che "sottoscrive" digitalmente o formalmente:

- ✓ la base giuridica del trattamento;
- ✓ se vengono trasferiti i suoi dati personali a Paesi terzi;
- ✓ il periodo di conservazione dei dati;
- ✓ il diritto di presentare un reclamo all'Autorità di controllo.

Inoltre, se il trattamento comporta processi decisionali automatizzati, l'informativa deve specificarlo.

L'informativa è quindi una comunicazione che serve per far conoscere all'interessato **come il titolare gestisce ed utilizza i dati** che lo riguardano e va consegnata al momento in cui la persona fornisce i suoi dati all'associazione.

I 3 diritti Privacy dell'interessato al trattamento

L'interessato pertanto con l'entrata in vigore delle nuove disposizioni in materia di Privacy, ha avuto il riconoscimento di alcuni **diritti** che enti ed imprese dovranno garantire. Questi Diritti, si riassumono in **3 punti fondamentali:**

1. ricevere una copia dei dati personali oggetto di trattamento (**DIRITTO DI ACCESSO**);
2. cancellazione dei propri dati personali (**DIRITTO ALL'OBLIO**), lì dove la conservazione non sia obbligatoria per ragioni di Leggi superiori e non sussistono legittimi motivi per mantenerli (p.es: non sono più necessari rispetto alla finalità per cui erano stati conferiti, ecc…);
3. **limitazione del trattamento**: è possibile raccogliere dati personali solo per finalità specifiche, esplicite e legittime dopo aver informato gli interessati su come si intende trattare i dati.

Che cos'è il principio dell'accountability con il nuovo GDPR?

Un principio molto importante introdotto dal nuovo Regolamento sulla Privacy è quello dell'***Accountability***.

Da regole statiche e uniformi per tutti a regole *adhoc* per ogni singola organizzazione con la c.d. Accountability.

Il modellino Standard da far firmare non basta più… Occorre una conoscenza della struttura e di come questa tratta i dati sensibili di coloro con cui interagisce.

L'accountability responsabilizza le imprese e gli enti in quanto non chiede loro di rispettare semplicemente una lista di regole statiche e già prestabilite.

Con il **GDPR** si prevede una **responsabilità** per l'Ente o l'impresa, quindi del **Responsabile del trattamento** con cui determinare e mettere in atto le misure tecniche ed organizzative ritenute adeguate in base alla propria realtà per garantire, ed essere in grado di dimostrare la **conformità alla normativa**.

Sulla base di questa premessa, occorre chiedersi:

- **Quali dati sensibili tratta l'associazione?**
- **Come tratta i dati l'associazione?**
- **Sono in grado di garantire la sicurezza dei miei dati?**
- **Sono in grado di dimostrare di aver ricevuto un consenso in maniera lecita e trasparente?**
- **Sono in grado di rimuovere agevolmente il consenso quando mi viene richiesto?**

Perché interessa il mondo del Non Profit?

L'applicazione del Regolamento non dipende dalla **dimensione** o dalla **natura** giuridica dell'impresa o ente ma dalla **natura dell'attività compiuta**.

Se si stima che il 50% delle aziende non sia in regola, probabilmente nell'ambito Non Profit la percentuale cresce sensibilmente.

Eppure il Non Profit è proprio uno dei settori in cui il **GDPR 2018** ha maggiore impatto perché queste organizzazioni sono proprio quelle che di sicuro hanno a che fare con **persone fisiche** e di conseguenza ne trattano i relativi dati, spesso sensibili.

Pensiamo ad esempio alle tante Organizzazioni di Volontariato, le Associazioni di Promozione Sociale (quali le AVIS, Croce Rossa, ecc.) la cui gestione del dato sensibile è parte integrante della finalità sociale dell'Ente medesimo (salute, benessere, ecc.).

Si ricorda infatti che, al nuovo impianto normativo, sono chiamati a conformarsi **tutti i titolari del trattamento, indipendentemente dalla loro natura giuridica**, dal settore merceologico d'appartenenza e dalle dimensioni dell'attività.

L'Ente Non Profit è titolare del trattamento ogniqualvolta svolge una sola operazione che si concretizza in un **trattamento di dati personali**.

Entro tale data, pertanto, anche gli enti e le organizzazioni non profit dovranno conformarsi poiché gestiscono dati sensibili oggetto di trattamento ai fini **della privacy** per numerosi soggetti, quali:

- i propri dipendenti;
- i collaboratori;
- i volontari;
- i donatori;
- i beneficiari in genere delle loro attività.

Tali Enti Non Profit dovranno procedere ad adeguarsi a tale nuova normativa al pari, se non in misura maggiore, delle Società commerciali.

E’ necessario rivedere l’organizzazione interna dell’ente no-profit?

E’ sempre importante verificare ed, eventualmente rivedere, le autorizzazioni al trattamento dei dati con il quale il titolare del trattamento abilita i propri dipendenti o collaboratori a trattare i dati nell’ambito della sua organizzazione e per le finalità della stessa. Senza l’autorizzazione il trattamento dei dati non è legittimo.

In questo documento devono essere presenti le seguenti indicazioni:

- l’ambito del trattamento autorizzato;
- le istruzioni per i trattamenti;
- l’uso dei dispositivi e le misure di sicurezza da osservare.

Il Registro dei Trattamenti

Importante novità è la predisposizione del **Registro dei trattamenti,** tenuto a cura dell’incaricato, che, seppure obbligatorio solo per determinati soggetti, è fortemente consigliato al fine di tenere costantemente monitorati i flussi e quindi i rischi.

La sua funzione è prevalentemente descrittiva ed il suo contenuto deve fornire un quadro aggiornato dei trattamenti in essere all’interno dell’organizzazione, indispensabile per ogni valutazione ed analisi del rischio.

Potrà essere utile anche predisporre un’ulteriore documento, denominato **Valutazione di impatto privacy (o DPIA)** che rappresenta un’analisi dei rischi generati in concreto dal trattamento dei dati, soprattutto se il trattamento prevede l’uso di nuove tecnologie.

L’analisi dovrà:

- considerare l’intero ciclo di vita dei dati, dalla raccolta alla cancellazione;
- descrivere in dettaglio tutte le operazioni di trattamento;
- descrivere le misure previste per affrontare i rischi connessi al trattamento;
- indicare le garanzie e le misure di sicurezza adottate per ridurre il rischio;
- essere formalizzata in un documento.

E’ opportuno anche prestare maggiore attenzione alla sicurezza dei sistemi informatici?

Le misure di sicurezza informatica devono certamente garantire un livello di sicurezza adeguato al rischio del trattamento.

Non esiste quindi un obbligo generalizzato di adozione di misure minime di sicurezza, poiché la valutazione sarà rimessa, caso per caso, al titolare ed al responsabile in rapporto ai rischi specificatamente individuati.

In ogni caso, tutti i titolari dovranno notificare all’Autorità di Controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore**, se da tale violazione possano ragionevolmente derivare rischi.

In cosa consiste la nuova figura del DPO (Responsabile della protezione dei dati)?

E' obbligatoria solo in alcuni casi:

- Se il titolare è un soggetto pubblico;
- Se l'attività principale del Titolare consiste in trattamenti che, per loro natura, ambito di applicazione o finalità comportano il monitoraggio regolare e sistematico degli interessati "su larga scala";
- Se l'attività principale del Titolare consiste in trattamenti regolari e sistematici di dati particolari o giudiziari.

La nomina del **DPO** non dipende dall'entità dell'ente, ma dalla **tipologia di trattamento effettuata e dal rischio cui si espongono i dati**.

Deve essere un soggetto esterno all'azienda, deve avere requisiti di professionalità e di esperienza commisurati alla sensibilità, complessità e quantità di dati trattati e deve godere di indipendenza ed autonomia di spesa

E' una funzione aziendale di informazione, consulenza, sorveglianza e di collegamento con il Garante e con gli interessati.

Quali sono le sanzioni?

Mentre rimangono invariate le **sanzioni penali**, le **sanzioni pecuniarie** amministrative subiranno un **deciso incremento**.

Tenendo conto delle esigenze delle micro, piccole e medie imprese e organizzazioni, le sanzioni amministrative dovranno essere **effettive, proporzionate e dissuasive** e nell'applicazione delle sanzioni le Autorità Garanti dovranno valutare il tipo e durata della violazione, le misure di sicurezza adottate dal titolare, la natura doloso o colposa della condotta.

Sanzioni Amministrative per violazioni Privacy

- **fino a 10 milioni di euro** per i singoli;
- per le imprese fino al **2% del fatturato** mondiale totale annuo dell'esercizio precedente, se superiore;

- **fino a 20 milioni** per i singoli;
- **per le imprese fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.

Sanzioni penali per violazioni Privacy

Le sanzioni penali rimangono di competenza di ogni singolo Stato, che deve predisporre sanzioni "effettive, proporzionate e dissuasive",

il Considerando (149) recita che: "Gli Stati membri dovrebbero potere stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento.

Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia.

Regolarizzare la Privacy (GDPR) dell'Ente Non Profit in 6 passi.

L'Ente Non Profit per stabilire quali azioni intraprendere per regolarizzare e mettere a norma di Legge l'organizzazione, dovrà affrontare alcuni approfondimenti riguardo la propria natura, **l'analisi dei dati sensibili** trattati e la **modalità attraverso la quale questi sono trattati** nella propria organizzazione.

Vi sottoponiamo una scaletta di **6 punti** più importanti da affrontare.

1. Effettuare **un'analisi** per individuare la **tipologia di dati raccolti**, i tipi di trattamenti effettuati e le finalità per le quali i dati sono raccolti dall'associazione;
2. Individuare **CHI** tratta i dati e aggiornare le nomine;
3. Dotarsi di **procedure interne** per limitare al massimo i rischi connessi al trattamento dei dati particolari;
4. Dotarsi di **sistemi IT** adeguati a limitare al massimo i rischi connessi al trattamento dei dati;
5. Predisporre **informative aggiornate** ed adeguate;
6. Implementare **sistemi efficaci per la raccolta del consenso** per il trattamento di dati particolari.

Per info e approfondimenti:

Asso360 Srl
Comunanza (AP)
www.asso360.it

Centro Studi Finanza & Persona
OAdvisory

Via G. Mercalli, 13

00197 ROMA

Tel: +39 06 95020121