Spettabile

Associazioni
Loro sedi

Venezia, 21 Maggio 2018

Oggetto: GDPR – General Data Protection Regulation

A partire dal 25 maggio 2018 entrerà in vigore, a seguito del Regolamento UE/2016/679, la **GDPR – General Data Protection Regulation**, cioè l'aggiornamento della normativa sulla Privacy che prevede pesanti sanzioni, anche sotto il profilo penale, per chi non la rispetterà. Il cambiamento riguarderà anche le associazioni.
Con la presente, in collaborazione con C.S.A. Srl, vi inviamo un breve riassunto della normativa e una check list da restituire al fine di valutare l'opportunità della necessaria documentazione che deve essere presente all'interno del sodalizio.

In sintesi:

Il principio di accountability

In base al principio di ***accountability*** introdotto dal GDPR (tradotto in italiano con il termine "responsabilizzazione"), i titolari del trattamento devono **mettere in atto tutte le misure tecniche e organizzative necessarie** per assicurare, ed essere in grado di dimostrare, che la raccolta e l'utilizzo dei dati siano conformi alle nuove regole.
A integrare questo approccio basato sulla valutazione del rischio intervengono i principi di ***privacy by design*** **e** ***privacy by default***. Si tratta di due concetti innovativi che impongono l'adozione di misure di protezione **fin dalla fase di progettazione del trattamento**, oltre a prescrivere un utilizzo che si limiti, per impostazione predefinita, ai soli dati necessari a rispondere alle finalità specifiche della gestione dei dati.

Kira srl
consulenza alle associazioni
Mestre, Via F. Baracca, 39
30173 Venezia (Ve)

www.kirasrl.it
info@kirasrl.it
tel. 041-5947844
fax 041-5947836

C.F. e P. IVA. 03447670278
C.C.I.A.A. 03447670278
Reg. Impr. VE 03447670278
Cap. Soc. Euro 12.000,00 i.v.

La valutazione d'impatto

Il **DPIA (Data Protection Impact Assessment,** (valutazione d'impatto sulla protezione dei dati) è forse l'operazione più importante da effettuare per rispondere al principio di accountability. La valutazione del rischio conseguente a un ipotetico *data breach* (fuoriuscita di dati) rappresenta un **elemento fondamentale per la corretta gestione di tutto il ciclo del trattamento**, fin dalla predisposizione dei mezzi utili al trattamento stesso.

Per questo, in particolari casi quali la sorveglianza sistematica su larga scala, il trattamento di particolari tipologie di dati o nel caso di profilazione ad alto rischio, il Regolamento prescrive **una valutazione preventiva e sistematica delle finalità e della necessità del trattamento.** In relazione a questa vanno indicate tutte le misure e le garanzie previste per una adeguata protezione dei dati personali trattati.

In caso di data breach (fuoriuscita di dati)

Se l'esame delle possibili fonti di rischio non è stato sufficiente ad evitare il verificarsi di una violazione dei dati personali, **il titolare del trattamento ha il dovere di comunicare la violazione all'autorità di controllo** (il Garante della privacy nazionale) entro 72 ore dal momento in cui ne è venuto a conoscenza.

Nel caso in cui la stessa violazione costituisca un **pericolo per le libertà e i diritti degli interessati**, anche ad essi dovrà essere fornita adeguata comunicazione.

Diritti di controllo sui propri dati

Non soltanto il Regolamento compensa questo vantaggio con una serie di limitazioni (in particolare il **principio di minimizzazione**) che di fatto obbligano il titolare ad utilizzare la minor quantità di dati e il minor periodo di tempo possibili per le finalità del trattamento, ma **amplia anche il ventaglio di diritti dell'interessato**.

Il GDPR mette qualunque persona fisica nella condizione di compiere un consapevole esercizio dei poteri di controllo sui propri dati, garantendogli il **diritto all'informazione**, il **diritto all'accesso, alla rettifica e alla cancellazione** dei dati che lo riguardano, il **diritto alla limitazione del trattamento** e il **diritto di opposizione**.

Diritto alla portabilità dei dati

Una novità assoluta è poi rappresentata dal **diritto alla portabilità dei dati**, che consente all'interessato di richiedere al titolare i propri dati in **formato strutturato** e leggibile da un elaboratore automatico, così da poterli **trasferire da un servizio ad un altro**.

COSA FARE

1) E' da compilare, in casi selezionati, la **DPIA** (Data Protection Impact Assesment, o valutazione d'impatto sulla protezione dei dati). Questo rappresenta lo strumento base per censire i rischi privacy.

2) Registro dei trattamenti dei dati

La tenuta del registro è un **obbligo che non si applica alle imprese e organizzazioni con meno di 250 dipendenti,** a meno che il trattamento non sia occasionale o ad alto rischio, o includa particolari categorie di dati (ad esempio i dati sensibili, ovvero **relativi alla salute** o alla vita sessuale, genetici, giudiziari e biometrici).

In sostanza, chi ha dipendenti, avendo a disposizione dati sensibili quali quelli relativi alla salute (vedi, ad esempio, le assenze per malattia), non gode dell'esenzione, come pure, peraltro, chi non ha dipendenti, ma ha, con clienti, fornitori o altri terzi, rapporti non occasionali.

In ogni caso, quindi, chi tratta dati di carattere sanitario o giudiziario è obbligato alla tenuta del registro

3) Designazione del Data protection officer (DPO o responsabile per la protezione dei dati o RPD)

Bisogna nominare, in casi selezionati, il **Responsabile della Protezione dei dati (RPD).**

La designazione del Data protection officer non è obbligatoria per tutti i titolari e i responsabili, ma solo per:

1. amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

2. tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati **su larga scala;**

3. tutti i soggetti la cui attività principale consiste nel trattamento, **su larga scala**, di dati sensibili**, relativi alla salute** o alla vita sessuale, genetici, **giudiziari** e biometrici.

Ulteriori casi di designazione obbligatoria possono essere individuati dal legislatore.

Soggetti esentati dalla nomina del RPD

La designazione del responsabile del trattamento non è obbligatoria in relazione a trattamenti effettuati da:

- liberi professionisti operanti in forma individuale;
- agenti, rappresentanti e mediatori operanti non su larga scala;
- imprese individuali o familiari;
- piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

Per ulteriori informazioni, vi chiediamo di compilare la check list allgato che provvederemo ad inoltrare a C.S.A. Srl che vi fornirà i chiarimenti necessari.

Cordiali saluti.

Kira Srl

Kira srl
consulenza alle associazioni
Mestre, Via F. Baracca, 39
30173 Venezia (Ve)

www.kirasrl.it
info@kirasrl.it
tel. 041-5947844
fax 041-5947836

C.F. e P. IVA. 03447670278
C.C.I.A.A. 03447670278
Reg. Impr. VE 03447670278
Cap. Soc. Euro 12.000,00 i.v.