IMPATTO DEL GDPR SULLE PRO LOCO DEL PIEMONTE

OBBLIGATORIA DAL 25/05/2018

Per “GDPR” si intende il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Sommario

Sintesi della normativa

ELEMENTI DI BASE

Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, la normativa è entrata in vigore il 24 maggio 2016, ma la sua attuazione avverrà, a distanza di due anni, **quindi dal 25 maggio 2018**.

Per chi si chiede se ci sarà una proroga al regolamento, la risposta è quasi certamente no!

Le Pro Loco del Piemonte hanno bisogno di spiegazioni concrete per capire come muoversi in questo nuovo ambito e sapere se hanno disponibili tutti gli elementi per definire un corretto piano di adempimento alla nuova normativa.

Le Pro Loco dovranno proteggere i dati personali dei clienti, dei soci, dei fornitori e dei propri dipendenti rispettando i canoni di sicurezza imposti.

BASE GIURIDICA DEL TRATTAMENTO DEI DATI

Il nuovo regolamento pone l'accento sul principio della trasparenza, in un'ottica di rispetto della finalità. Occorre, quindi, valutare attentamente gli scopi del trattamento, in modo da stabilire correttamente quali dati possono essere trattati e quali no (principio di essenzialità dei dati).

Con il GDPR, inoltre, i titolari del trattamento dovranno identificare la base giuridica del trattamento (ad esempio il consenso dell'interessato) **e documentarla**, in quanto in relazione alla base giuridica possono variare i diritti. Ad esempio, **è stato rafforzato il diritto alla cancellazione** nel caso di trattamenti basati su consenso.

I PASSI ESSENZIALI PER DIFENDERE IL DATO

- Primo passo – Avere sempre una mappatura su un registro dei dati e del trattamento all'interno della realtà della Pro Loco. Fare cioè il tracking del dato, di come il questo viene raccolto, dove viene custodito ma anche come viaggia, quando muore e per quale periodo viene conservato.

- Secondo passo – Comprendere se è necessario attuare un DPO, cioè una persona all'interno della realtà che sia presidio, che anche se obbligatorio solo per le realtà più ampie, può essere comunque utile.

- Terzo passo – Gestire correttamente la violazione del dato, probabilmente la minaccia più importante che il regolamento evidenzia. Capire infine quando è il caso di segnalare all'utente delle anomalie che lo riguardano.

Cosa deve fare la Pro Loco per il Web

ESEMPI PRATICI

Uno degli aspetti più importanti di questa normativa è **il consenso.** L'UE ha affermato che è necessario "ottenere il loro chiaro consenso per elaborare i dati". Ciò **significa che gli utenti devono dire esplicitamente di sì**, non solo avere la possibilità di dire di no.

Ecco un esempio: Quando gli utenti arrivano in una pagina web e trovano un modulo di iscrizione alle newsletter, probabilmente, troveranno una casella di controllo che legge: "[x] Sì, voglio registrarmi per la tua lista di e-mail!"

Se la casella è selezionata per impostazione predefinita, **è un errore**. Questo sta dando loro solamente la possibilità di rinunciare e non è ciò che dice la regola, in realtà. Gli utenti **devono scegliere esplicitamente** di condividere le loro informazioni con te.

La stessa cosa vale per le sezioni dei commenti se sono attivati nel sito web che iscrivono automaticamente gli utenti al thread dei commenti o qualsiasi altro tipo di contatto automatizzato che non sia direttamente avviato dall'utente.

Se sulla pagina web si utilizza **pubblicità di profilazione** (elaborazione dei dati relativi a uno o più clienti o utenti, allo scopo di suddividerli in gruppi omogenei in base a gusti, interessi e comportamenti.) o comunque random gestita da aziende di marketing esterne come Google (AdWord, Pay for click ecc) ricordarsi di **informare l'utente e richiedere un consenso esplicito**.

In estrema sintesi l'obiettivo primario deve essere quello di non prendere nulla per impostazione predefinita. E consigliabile prendere il meno possibile, lo stretto necessario e **ottenere sempre un permesso esplicito**.

RICHIEDI SOLO LE INFORMAZIONI NECESSARIE

Se non si ha bisogno del loro nome, meglio non prenderlo. A volte basta la loro e-mail per completare il tuo lavoro.

Questo non vuol dire che non puoi chiedere altre informazioni. Il GDPR dice semplicemente che bisogna dire alla gente perché se ne ha bisogno. Se stai chiedendo il loro nome e cognome, digli perché. Se hai un modulo (o form) includi una nota sotto / accanto all'etichetta principale, quindi se disponi di un campo per i numeri di telefono, specifica *"in modo che i nostri rappresentanti del servizio possano contattarti più velocemente.*"

Inoltre, quando chiedi informazioni, l'UE dice che devi rivelare "chi sei, per quanto tempo sarà archiviato e chi lo riceverà". Per quanto riguarda come e quando devi rivelare queste cose, quello può differire. La comunicazione primaria è che devi dire chi sei nello stesso momento in cui fai la richiesta dei loro dati.

Basta una frase che spieghi chi sei, una sola riga che afferma che *"I dati di questo sito web sono gestiti da M.Rossi, Titolare del trattamento dei dati per la Pro Loco di...".* O anche qualcosa come *"I dati inviati da questo modulo verranno utilizzati dalla Pro Loco di... e nessun altro"* funzionerà.

Ciò significa che il tuo modulo di contatto, il modulo di iscrizione alle newsletter, ovunque gli utenti potrebbero fornirti le loro informazioni, devono identificare chiaramente chi sei e lo scopo della raccolta dei loro dati.

INFORMATIVA SULLA PRIVACY

Per quanto riguarda le altre parti delle clausole di conservazione dei dati del GDPR, è possibile includere, nei Termini di servizio o Norme sulla privacy i dettagli sui motivi, sulle modalità, su dove vengono conservati e su chi è il Titolare del trattamento dei dati.

Il passaggio è importante e duplice: in primo luogo, assicurati che l'informativa sulla privacy siano conformi allo stesso GDPR. E in secondo luogo, creare campi obbligatori espliciti su ogni modulo che indica l'accettazione di entrambi i documenti prima di elaborare qualsiasi cosa. Le caselle di controllo sono soddisfacenti e i campi di testo in cui gli utenti possono digitare "Sono d'accordo" sono ancora migliori (anche se antipatici).

Suggerirei di aggiungere un paragrafo nei Termini di servizio per accettare l'Informativa sulla privacy come termine da collegare direttamente al modulo. Quindi, nell'Informativa sulla privacy, è meglio aggiungere un paragrafo che discute esattamente come il tuo sito gestisce i dati in conformità al GDPR. Nello specifico, si dovrà fornire istruzioni dettagliate spiegando ognuna delle seguenti informazioni.

1. Come accedere e scaricare una registrazione completa di tutti i dati che hai su di loro
2. Il processo attraverso il quale gli utenti possono cancellare completamente i propri dati dai tuoi archivi (e non semplicemente annullare l'iscrizione, ecc.) questo fa parte delle leggi sul "diritto all'oblio" precedentemente approvate nell'UE
3. Esattamente come informerai gli utenti di violazioni dei dati, se mai accadessero
4. Spiegazioni dettagliate su chi sei, su come usi i dati, chi ha accesso e quanto a lungo lo trattieni

Ora è più importante che mai avere una politica sulla privacy in atto. Era già abbastanza importante prima perché Google voleva che tutti ne avessero uno. E quell'importanza dal 25 maggio 2018 salirà in maniera esponenziale.

RENDERE IL PROPRIO SITO SICURO

Acquistare un **certificato SSL** per il proprio sito. Il certificato si basa su un processo di crittografia a chiave pubblica, per garantire la sicurezza della trasmissione dei dati su internet. Il suo principio consiste nello stabilire un canale di comunicazione sicuro (cifrato) tra due terminali (un client e un server) dopo una tappa di Autenticazione. La semplice iscrizione alla newsletter in un sito non protetto rende intercettabile esternamente l'indirizzo e-Mail.

IN BREVE

- Usa un linguaggio semplice.
- Dì loro chi sei quando richiedi i dati.
- Spiega perché stai elaborando i loro dati, per quanto tempo sarà archiviato e chi lo riceverà…
- Ottieni il loro chiaro consenso per elaborare i dati.
- Controllare il limite di età per il consenso dei genitori.
- Predisporre la dichiarazione di maggiore età.
- Consenti alle persone di accedere ai propri dati per consegnarli a un'altra società.
- Informare le persone di violazioni dei dati se c'è un serio rischio per loro.
- Dai alla gente il "diritto all'oblio". Ossia cancellare i dati personali se lo chiedono.
- Dare alle persone il diritto di rinunciare al marketing diretto che utilizza i loro dati.
- Usa ulteriori salvaguardie per informazioni su salute, razza, orientamento sessuale, religione e convinzioni politiche.
- Se si utilizza la profilazione: Informa i tuoi clienti; assicurati di avere una persona, non una macchina, che controlla il processo se l'applicazione web finisce in un rifiuto. Offrire sempre al richiedente il diritto di contestare la decisione.
- Prendere accordi legali quando si trasferiscono dati in paesi che non sono stati approvati dalle autorità dell'UE.
- Esiste l'obbligo di non cambiare in corso d'opera lo scopo per il quale i dati sono stati raccolti. Ciò implica che per ogni utilizzo dei dati diverso dall'originale sarà necessario ottenere un nuovo consenso dei soggetti coinvolti.
- Le Pro Loco dovranno quindi disporre di tecnologie per cancellare in tempo reale dati su richiesta dei soggetti.

Cosa fare per i rapporti fuori dal web

MODULISTICA CARTACEA O ELETTRONICA

Predisporre moduli di consenso cartacei o elettronici per la conservazione ed il trattamento dei dati di tutti i soggetti che abbiano rapporti con la Pro Loco: **Clienti, Fornitori, Dipendenti o Collaboratori in genere**.

Ecco un esempio: Il GDPR richiede alle organizzazioni di dettagliare quali sono le informazioni sui dipendenti, chi ha accesso alle informazioni e dove risiede l'informazione. La mancata conformità può essere costosa, le multe potrebbero essere molto ingenti. Molti dati personali vengono ricevuti durante il selezione e reclutamento del personale. CV, moduli di domanda, presentazioni personali ecc.

- Qual è la politica della Pro Loco per la memorizzazione e la gestione di tali dati?
- Quando un potenziale dipendente arriva per il colloquio, probabilmente verranno prese ulteriori informazioni personali, come ad esempio le foto. Come potete dimostrare che la persona intervistata ha dato il consenso per questo?
- Se poi non verranno assunti, che cosa si fa con questi dati?
- Per quanto tempo devono essere gestiti?
- Quando un candidato viene assunto e diventa un dipendente, hai un processo chiaro per spostare i dati dal registro di reclutamento del personale al registro dei dipendenti?
- Oppure le informazioni risiedono in entrambi?

Insomma anche in questo caso si dovranno predisporre moduli di consenso esplicito per l'uso di tutte queste informazione e ricordarsi di apportare le dovute variazioni sul registro dei trattamenti.

MODULISTICA PER IL TESSERAMENTO DEI SOCI

Predisporre moduli di consenso cartacei o elettronici per la conservazione ed il trattamento dei dati di tutti i soci della Pro Loco, si dovrà specificare il perché si ha bisogno dei loro dati, dove si conserveranno, chi è il titolare del trattamento e i dati di contatto dello stesso, l'uso che si farà di questi dati e se verranno condivisi con altri. Ricordate che per l'uso di marketing si dovrà dare la possibilità al socio di poterla rifiutare.

L'adesione al servizio di newsletter, però, deve essere distinta dal consenso a ricevere comunicazioni promozionali, e l'aver richiesto di ricevere periodicamente un notiziario circa le attività e i servizi della Pro Loco non implica che il socio abbia manifestato la volontà di ricevere comunicazioni commerciali in ordine ai servizi resi dall'Associazione o, peggio, da terzi. Né il conferimento dei dati per ricevere le newsletter potrebbe abilitare il Titolare del trattamento a fornire ulteriori, diverse comunicazioni.

In altre parole **se si vuole effettuare marketing**, dunque, **occorre acquisire un apposito consenso**.

Di cosa dovranno dotarsi le Pro Loco

REGISTRO DEI TRATTAMENTI

La tenuta del registro dei trattamenti è prevista dall'articolo 30 del regolamento generale europeo, ed è considerata indice di una corretta gestione dei trattamenti.

L'onere della tenuta del registro è a carico del titolare e, se nominato, del responsabile del trattamento. La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e ad una corretta pianificazione dei trattamenti. Per cui le autorità invitano tutti i titolari a dotarsene, eventualmente inserendo negli stessi ogni elemento utile, anche oltre a quelli minimi previsti dalle norme.

Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e va esibito all'autorità di controllo (Garante) in caso di verifiche. **Sono esentate dall'obbligo di tenuta del registro le imprese o le organizzazioni con meno di 250 dipendenti.**

Anche se non obbligatorio per le Pro Loco (non credo esistano Pro Loco con 250 dipendenti) il Garante per la protezione dei dati personali, nella sua Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali ritiene che: *"il registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali"*, invitando tutti i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro.

Il registro deve contenere come minimo queste informazioni:

A. nome e i dati di contatto del titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
B. le finalità del trattamento;
C. una descrizione delle categorie di interessati e delle categorie di dati personali;
D. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
E. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti, la documentazione delle garanzie adeguate;
F. i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
G. una descrizione generale delle misure di sicurezza tecniche e organizzative.

Come detto poc'anzi, il registro dei trattamenti è uno strumento fondamentale per mappare i flussi di dati all'interno dell'organizzazione. Infatti, potremmo aggiungere al nostro registro una colonna in cui indicare quali database contengono le informazioni trattate, quali software le processano, quali server sono coinvolti in tali trattamenti, arrivando persino a indicare quali profili sono autorizzati al loro trattamento.

È importante capire sin da subito, però, che il registro dei trattamenti non è un documento che una volta redatto può rimanere fermo e immutabile per sempre, dev'essere inteso come un vero e proprio strumento di lavoro, e come tale deve essere modificato e deve essere mantenuto aggiornato, e sempre attuale.

Per raggiungere questo scopo è fondamentale innanzitutto individuare, all'interno dell'organizzazione, i soggetti che hanno la più ampia visione delle attività di trattamento e coinvolgerli nella redazione e aggiornamento del registro dei trattamenti, responsabilizzandoli sull'importanza di tale attività. È necessario renderli edotti dei vantaggi e del valore aggiunto che una gestione trasparente dei flussi di dati personali rappresenta per l'organizzazione.

Il registro dei trattamenti dovrebbe essere gestito in maniera centralizzata, garantendo l'accesso a tutte le persone coinvolte nel suo mantenimento onde evitare la proliferazione di copie che renderebbero difficile identificare la versione più aggiornata.

RACCOMANDAZIONI

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento.

In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di modulistica.

Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara.

SANZIONI

La mancata osservanza di queste linee guida determinerà una sanzione.
Fino a 20 milioni di euro o il 4% del tuo fatturato annuale, quindi un bel po' di soldi.

Informazioni sull'autore

VINCENZO DI LORENZO

e-Mail vidilorenzo@outlook.it

Informazioni sull'organizzazione

Comitato Regionale Unpli Piemonte

Via Buffa di Perrero, 1 - 10061 - Cavour (To) - Italy

Tel. 0121.68.255

Fax 0121.609.448

e-Mail unplipiemonte@unplipiemonte.it

www.unplipiemonte.it