GDPR, cosa devono fare le organizzazioni No-Profit

19 novembre 2018, Galliate (No)

SPEDI
servizi per l'informatica

Sommario

- Cos'è il GDPR
- I principi del GDPR
- Cosa c'è di nuovo (rispetto al D.Lgs. 196/2003)
- Tipologia dei dati
- Le figure coinvolte
- Nomine
- L'informativa
- Il consenso
- Il registro dei trattamenti
- Consigli per le newsletter
- Conclusioni

SPEDI
servizi per l'informatica

Cos’è il GDPR

- Il General Data Protection Regulation (Regolamento UE 2016/679) disciplina la tutela delle **persone fisiche**, con riferimento ai dati personali e alla libera circolazione dei dati.
- È diventato operativo dal **25 maggio 2018** e si applica a tutte le organizzazioni che gestiscono, custodiscono, trattano, trasmettono o operano in altro modo i dati personali di persone fisiche, che sono **cittadini dell’Unione Europea**.

- **Il regolamento non si applica:**
  - *Per le persone giuridiche*
  - *In ambito personale o domestico*

SPEDI
servizi per l’informatica

I principi del GDPR

- Vengono dettate le regole, ma c'è discrezionalità sul se, cosa e come fare
- Onere di dimostrare le ragioni delle decisioni prese
- Gli adempimenti cambiano in funzione dei dati e delle attività svolte
- Non importa come vengono trattati i dati (cartaceo, elettronico, videosorveglianza): i dati personali sono soggetti agli obblighi di protezione stabiliti dal regolamento

Cosa c’è di nuovo
rispetto al D.Lgs. 196/2003

- Diritto all’oblio
- Diritto alla portabilità dei dati
- Privacy by default e privacy by design
- Registro dei trattamenti
- Valutazione d’impatto
- Obbligo di notifica e comunicazione del data breanch
- Misure tecniche adeguate
- Responsabile della protezione dei dati (RPD)
- Entità delle sanzioni

SPEDI
servizi per l’informatica

Tipologia dei dati (1/2)

- Cosa si intende per «dato personale»?
  - Art. 4.1 qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente.
  - Esempi:
    - *Nome e cognome*
    - *Indirizzo*
    - *E-mail (con nome e cognome)*
    - *Numero della carta d'identità*
    - *Numero di telefono*
    - *Targa auto*

Tipologia dei dati (2/2)

- Cosa si intende per «dato sensibile»?
  - Art. 9 dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, biometrici, relativi alla salute o vita sessuale o all'orientamento sessuale, dati relativi a condanne penali e reati o a connesse misure di sicurezza.
  - Esempi:
    - *Dati biometrici come carta d'identità, patente, passaporto*

Le figure coinvolte

- Interessato
  - *Esempio: Socio, Fornitore, Cliente, Dipendente*
- Titolare del trattamento
  - *Esempio: Presidente*
- Responsabile del trattamento
  - *Esempio: Direttivo, Socio, chi ricopre particolare incarico*
- Responsabile della protezione dei dati (RPD), se previsto

Nomine

- Responsabile del trattamento interno
  - *Esempio: Direttivo, Socio, chi ricopre particolare incarico*
- Responsabile del trattamento esterno
  - *Esempio: Commercialista, Informatico, chi ricopre particolare incarico*
- NOTA: per tutti gli organi istituzionali non occorre una nomina, ma è sufficiente citarli nel Registro dei trattamenti.

SPEDI
servizi per l'informatica

L’informativa

- L’art. 13 elenca le informazioni da fornire:
  - L’identità e i dati di contatto del Titolare del trattamento
  - Le finalità del trattamento cui sono destinati i dati personali e la base giuridica del trattamento
  - Il periodo di conservazione dei dati
  - L’esistenza del diritto dell’interessato a chiedere l’accesso, la rettifica, la cancellazione o la limitazione,
  - L’esistenza del diritto di revocare il consenso al trattamento
  - Se la comunicazione è un obbligo legale o contrattuale oppure un requisito necessario
  - Le conseguenze della mancata comunicazione dei dati
  - L’esistenza di un processo automatizzato

L’informativa - Esempio

I dati conferiti saranno trattati nel rispetto del GDPR garantendone la riservatezza e la protezione.

Il conferimento dei dati è necessario per l’instaurazione o il mantenimento del rapporto associativo e il raggiungimento delle finalità dell’associazione. I dati saranno utilizzati esclusivamente per lo svolgimento dell’attività istituzionale, ed in particolare si informa:

……..

……..

SPEDI
servizi per l’informatica

Il consenso

- L'art. 7: «la **richiesta di consenso** è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un **linguaggio semplice e chiaro**»
- Minori: è lecito se il minore ha almeno **14 anni**, altrimenti tale consenso deve essere dato dai genitori
- Dati sanitari: Il consenso non è necessario se i dati sono trattati da personale sanitario tenuto al rispetto del segreto professionale
- Se la Pro Loco intende utilizzare i dati del socio **per scopi diversi dal rapporto associativo** puro e semplice, sia pure ad esso connessi, e in particolare se intende passare a terzi (qualsiasi soggetto pubblico o privato diverso dalla Pro Loco) i dati del socio, anche per es. per una assicurazione infortuni nominale, deve avere un **CONSENSO SCRITTO SPECIFICO** (non generico) per ciascuna evenienza. In particolare porre attenzione ad avere il consenso quando poi al socio arriveranno comunicazioni commerciali.
- Se la Pro Loco utilizza i dati del NON socio, ottenuti attraverso un form su Sito Internet, oppure tramite contatto diretto dell'interessato, dovrà richiederne il consenso.
- Il consenso deve essere sempre dato in forma scritta e sono vietate le caselle prefincate.

SPEDI
servizi per l'informatica

Il registro dei trattamenti

- Il garante della privacy ha raccomandato a tutti gli enti, anche quelli non obbligati per legge, di tenere il registro dei trattamenti
- Cosa contiene
  - Quali dati trattiamo > Dati personali dei soci
  - La base giuridica > Condizioni contrattuali
  - Per quali finalità > Adempimenti associativi
  - Con quali modalità > Cartaceo / elettronico
  - Se trasferiamo i dati a terzi > Commercialista, ASL
  - Chi tratta i dati > Responsabile
  - L'analisi dei rischi > Misure di sicurezza adottate
  - Termine ultimo di cancellazione > Al termine del contratto

SPEDI
servizi per l'informatica

Consigli per le newsletter

- Controllare se esiste il consenso, se è conforme al GDPR e se possiamo dimostrarlo
- Fare pulizia delle liste
- Chiedere solo i dati strettamente necessari
- No a caselle già selezionate per iscriversi
- No a richieste di consensi generiche per più scopi
- Usare il protocollo SSL

SPEDI
servizi per l'informatica

Conclusioni

La scaletta dei lavori da fare

- Un’analisi per **individuare la tipologia dei dati** raccolti, i tipi dei trattamenti e le finalità
- Individuare chi tratta i dati e aggiornare le **nomine**
- Fare un’**analisi dei rischi** e dotarsi di procedure interne
- Dotarsi di **sistemi tecnologici adeguati** a limitare al massimo i rischi
- Aggiornare tutte le **informative** sulla privacy (tesseramento, sito, newsletter)
- Implementare sistemi efficaci per la raccolta del **consenso**

SPEDI
servizi per l’informatica

DOMANDE & RISPOSTE

SPEDI
servizi per l'informatica

- Sviluppo software
- Attività Sistemistica
- Consulenza ICT

- Viale Marconi 72/e - 13045 Gattinara (VC)
- info@spedi.it
- www.spedi.it
- 0163 835328

spedisrl @spedisrl_official @spedisrl

SPEDI
servizi per l'informatica