www.corocittadidesio.it

Regolamento Interno dell'Associazione di cultura musicale "Coro Città' di Desio"

LINEE GUIDA SULLA PROTEZIONE DEI DATI PERSONALI DELLE PERSONE FISICHE

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Maggio 2018

1. PREMESSA

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 (di seguito General Data Protection Regulation o **GDPR** o Regolamento) del Parlamento Europeo e del Consiglio che disciplina la protezione dei dati personali delle persone fisiche, nonché la libera circolazione di tali dati nell'Unione europea. Tale Regolamento, efficace dal 25 maggio 2018, abroga la precedente Direttiva 95/46/CE ed è direttamente applicabile in tutti gli Stati membri.

La normativa europea responsabilizza ciascun Titolare del trattamento all'attuazione degli opportuni interventi normativi, organizzativi e tecnologici, al fine di rispondere adeguatamente ai requisiti prescritti secondo un principio di accountability.

In particolare, deve conformarsi al Regolamento ogni trattamento di dati personali effettuato da Titolari o Responsabili del trattamento, che trattano dati personali di interessati che si trovano nell'Unione.

Il diritto alla protezione dei dati personali, o diritto alla privacy, costituisce un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea.

2. PRINCIPI GENERALI

L'Associazione attribuisce rilevanza strategica alla protezione dei dati personali delle persone fisiche con cui interagisce (soci, collaboratori, fornitori, professionisti, etc.), nella consapevolezza che tale protezione sia volta, in ultima analisi, a tutelare la persona umana e i suoi diritti fondamentali di libertà e dignità.

Il rispetto dei diritti e delle libertà delle persone rappresenta, infatti, un fattore identitario e valoriale. A tal fine ci si adopera "per la protezione delle persone, dei valori e dei beni, del patrimonio informativo e dei processi organizzativi interni in modo da fornire un servizio che soddisfi al massimo grado i requisiti di affidabilità, continuità e riservatezza"; assicura "la costante aderenza alle disposizioni di legge"; osserva "criteri di assoluta trasparenza nell'informare tutti sui loro diritti alla privacy e sulle modalità con cui trattiamo le loro informazioni personali".

In tale ottica, si dota di un modello (Regolamento Interno) finalizzato ad assicurare che i dati personali siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità (limitazione della finalità);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
- esatti e, se necessario, aggiornati adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);
- trattati garantendo un adeguato livello di sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

Il trattamento dei dati personali svolto dalle persone autorizzate al trattamento dei dati deve essere attinente e/o comunque connesso alle funzioni assegnate. Ogni accesso ai dati personali deve pertanto essere effettuato in esecuzione delle mansioni assegnate o sulla base di una richiesta dell'interessato.

La comunicazione di dati all'interno è consentita solo se sussiste una base giuridica che la legittimi (es.: adempimento obbligo legale, esecuzione di un contratto con l'interessato, consenso da parte dell'interessato).

La comunicazione dei dati a terzi per finalità diverse dall'obbligo legale o dall'esecuzione contrattuale o assicurativa, non è consentito.

3. RUOLI E RESPONSABILITA'

3.1 ORGANI

Gli Organi che compongono l'associazione sono responsabili, ciascuno secondo le proprie competenze e prerogative, di assicurare l'adeguato presidio del rischio di non conformità in materia di protezione dei dati personali ai quali l'Associazione potrebbe essere esposta.
Le competenze degli Organi Amministrativi sono descritti nello Statuto dell'Associazione e nei relativi Regolamenti che ne disciplinano il funzionamento. Nel fare rinvio a tali documenti, nel seguito sono riportati i soli compiti direttamente interessi alle nuove disposizioni del Regolamento.

3.2 TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento dei dati è l'entità nel suo complesso che esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento.
L'Associazione CORO CITTA' di DESIO è il ***"Titolare del trattamento***".

3.3 CONSIGLIO DIRETTIVO

I componenti del Consiglio Direttivo sono deputati alla gestione dei dati ciascuno secondo le attività a loro assegnate per il corretto svolgimento della vita associativa e delle finalità statutarie.
Il Consiglio Direttivo:

- approva la modulistica da utilizzare in materia di protezione dei dati personali e, a tal fine, approva il presente Regolamento;
- nomina il Responsabile del Trattamento dei Dati Personali;
- è tempestivamente informato in caso di gravi problemi per l'attività associativa derivante da violazioni della riservatezza, della disponibilità o dell'integrità dei dati personali;

3.4 RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Il Responsabile è designato dal "***Consiglio Direttivo"*** ed ha il compito di sorvegliare l'osservanza del GDPR da parte della Associazione, dei suoi Consiglieri, adottando opportuni controlli.

In particolare, il Responsabile del Trattamento dei Dati personali, provvede a:

- supportare il Consiglio Direttivo nella valutazione degli eventi di non conformità che possono costituire un Data Breach e la necessità di effettuare la notificazione al Garante per la Protezione dei Dati Personali e/o dare comunicazione agli interessati appena ne viene a conoscenza;
- portare all'attenzione del Consiglio Direttivo le questioni in tema di protezione dei dati personali considerate di particolare rilevanza e fornire a quest'ultimo un'informativa scritta quando si manifesta la necessità;
- gestire i riscontri scritti nei confronti del Garante per la Protezione dei Dati Personali e degli interessati a seguito di ricorsi, segnalazioni o reclami presentati a tale Autorità ed evadere le richieste di esercizio dei diritti degli interessati;
- eseguire i controlli annuali in materia di protezione dei dati personali e la congruità del presente documento con la normativa tempo per tempo vigente redigendo apposita relazione sul riscontro solo in caso di criticità riscontrate;
- eseguire l'archivio e la custodia della documentazione.

Il Responsabile del Trattamento dei Dati Personali viene designato dal Consiglio Direttivo, sino a revoca, nella persona di Fabio Motta.

3.5 INCARICATI

Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del "**Titolare del trattamento**" o del Responsabile del Trattamento dei Dati Personali attenendosi alle istruzioni impartite.
Vengono incaricati:

- Fabio Motta, Enrico Balestreri, Mattia Arienti, Cristian Chiggiato, Lauretta Villa, Ornella Colombo, Paolo Corti, quali componenti del Consiglio Direttivo sono nominati alla gestione dei dati ciascuno secondo le attività a loro assegnate per il corretto svolgimento della vita associativa e delle finalità statutarie,
- Mattia Arienti è nominata alla gestione dei dati del sito del CORO e tutti i social attivi,
- Mattia Arienti e Federico Arienti, Ciliberti Clara, Matilde De Vitis, Silvia Balestreri sono nominati alla gestione dei dati sui social,
- Lauretta Villa, Enrico Balestreri, Mattia Arienti, Cristian Chiggiato e Fabio Motta sono nominati alla gestione dei dati per svolgimento operazioni amministrative, contabili, fiscali e per l'espletamento delle formalità con Siae e Assicurazioni.

4. VERIFICA DELLA LICEITA' DEL TRATTAMENTO

Al fine di stabilire la liceità del trattamento, i Componenti del Consiglio Direttivo, identificano la base giuridica del trattamento tra:

- consenso;
- esecuzione di un contratto di cui l'interessato è parte, o esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- obbligo di legge cui è soggetta la Associazione;
- legittimo interesse del Titolare o di terzi cui i dati vengono comunicati, sempre che non prevalgano gli interessi o i diritti e le libertà fondamentali degli interessati.

5. GESTIRE LE TERZE PARTI E IL TRASFERIMENTO DEI DATI EXTRA UE

Per quanto riguarda il trattamento dei dati personali che la Associazione affida a terzi (inclusi commercialisti, consulenti, Associazioni di categoria, fornitori/terze parti ed eventuali subfornitori, se autorizzati), generalmente nell'ambito di contratti e di rapporti di collaborazione a vario titolo, oltre alla figura del Titolare del trattamento si individuano se necessario le figure del Responsabile del trattamento dei dati personali.

Prima di conferire a un terzo un incarico di natura contrattuale, o un incarico di collaborazione che possa comportare il trattamento di dati personali i Componenti del Consiglio Direttivo, effettuano una valutazione in merito al ruolo soggettivo da attribuire alla Terza Parte.

6. CANCELLARE I DATI

L'obiettivo è garantire che i dati vengano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati; dopodiché essi devono essere cancellati o resi anonimi.

La Associazione tratta i dati personali fino al conseguimento delle relative finalità e successivamente li conserva nel rispetto dei termini previsti dalle norme di legge in vigore. Una volta decorsi tali termini, i dati vengono spostati in archivi segregati il cui accesso è consentito alle sole funzioni autorizzate (es.: componenti del Consiglio Direttivo), con conseguente cancellazione degli stessi sugli applicativi; qualora la creazione di un archivio segregato sia tecnicamente troppo complessa o onerosa, i dati potranno essere mantenuti sugli applicativi con limitazione dell'accesso alle sole funzioni autorizzate.

7. GESTIRE GLI EVENTI DI NON CONFORMITA'

I componenti il Consiglio Direttivo forniscono assistenza e collaborazione al Responsabile del Trattamento dei Dati Personali (di seguito Responsabile del Trattamento) nella gestione degli eventi di non conformità, assicurando l'individuazione e l'implementazione delle necessarie azioni correttive.

Qualora l'evento di non conformità configuri un "Data Breach" - ossia un incidente di sicurezza che comporta una violazione della riservatezza, della disponibilità o dell'integrità dei dati personali - il Responsabile del Trattamento ne valuta gli impatti in termini di rischio per i diritti e le libertà delle persone fisiche ai fini degli obblighi di notifica all'Autorità di controllo e di comunicazione agli interessati. Provvede a individuare e qualificare i rischi/danni connessi alla violazione dei dati personali e a valutarne il livello dando comunicazione scritta al Consiglio Direttivo.

Una volta individuato un Data Breach il Responsabile del Trattamento provvede a notificarlo all'Autorità di controllo **entro 72 ore** dal momento in cui il Titolare ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Se il rischio risulta elevato si procede anche alla comunicazione agli interessati coinvolti, al fine di fornire loro informazioni precise sulle azioni per proteggersi dalla violazione.

Il riferimento ai diritti e alle libertà degli interessati va inteso in primo luogo come violazione del diritto alla privacy (es: perdita del controllo dei dati personali, discriminazione, furto di identità,

pregiudizio alla reputazione, violazione della riservatezza, o qualsiasi altro danno economico o sociale significativo per la persona interessata), ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero o la libertà di movimento.

Per tutti gli eventi di Data Breach, a prescindere dall'avvenuta notifica all'Autorità, il Responsabile del trattamento conserva la documentazione raccolta degli eventi critici per documentare la violazione dei dati personali, le conseguenze, le azioni di mitigazione effettuate e, eventualmente, le motivazioni che hanno giustificato la mancata notifica.

8. INFORMARE GLI INTERESSATI E ACQUISIRE IL CONSENSO

E' necessario comunicare agli interessati tutte le informazioni necessarie per garantire un trattamento corretto e trasparente tramite un'informativa redatta in forma concisa, trasparente, intelligibile, facilmente accessibile e con un linguaggio semplice e chiaro.

Per questi motivi, è stato predisposto un testo di informativa specifica, per ciascuna tipologia di interessato: i soci, i collaboratori etc., per acquisire i relativi consensi, ogni qual volta risulti necessario.

L'informativa predisposta:

- viene fornita all'interessato per iscritto (o in formato elettronico, in caso di servizi online) nel momento in cui i dati personali sono ottenuti, sempreché i dati siano raccolti direttamente presso l'interessato stesso (es.: in fase di richiesta di ammissione a socio);

Non deve essere fornita informativa all'interessato se e nella misura in cui:

- l'interessato dispone già delle informazioni.

I consensi raccolti precedentemente all'emanazione del Regolamento (UE) 2016/679 rimangono validi se hanno tutte le caratteristiche sopra individuate.

9. GESTIONE DEI DIRITTI DELL'INTERESSATO

L'obiettivo è di garantire agli interessati l'effettivo esercizio dei diritti previsti dal Regolamento:

a) diritto di accesso, ossia il diritto di ottenere la conferma che sia o meno in corso un trattamento di propri dati personali e, in caso affermativo, di ottenerne l'accesso o una copia;
b) diritto di rettifica/integrazione dei dati trattati al fine di garantire che siano sempre esatti e aggiornati;
c) diritto alla cancellazione dei dati personali oggetto di trattamento;
d) diritto di limitazione di trattamento per il periodo di tempo necessario a tutelare i diritti dell'interessato;
e) diritto alla portabilità dei dati, ossia il diritto di:
    1. ricevere i dati personali trattati di conservarli in vista di un utilizzo ulteriore per scopi personali;
    2. trasmettere i dati personali ad un altro Titolare del trattamento;
f) diritto di opposizione ai trattamenti basati su un legittimo interesse del Titolare;
g) diritto alla revoca del consenso, che deve essere esercitabile con la stessa facilità con cui il consenso è stato prestato;
h) diritto di esprimere la propria opinione

i) diritto di ottenere una spiegazione delle decisione assunte e di contestare la decisione.

Entro un mese dal ricevimento della richiesta il Responsabile del Trattamento, fornisce risposta scritta all'interessato ovvero lo informa, sempre per iscritto, che, in virtù della complessità della richiesta, verrà fornito riscontro entro i successivi due mesi.

Qualora dalla richiesta non sia possibile accertare l'identità dell'interessato si provvede a richiedere le evidenze necessarie (a seconda dei canali utilizzati, esibizione o invio di una copia di un documento d'identità in corso di validità). In questo caso, i tempi per la risposta decorrono dal momento del ricevimento della documentazione integrativa ai fini dell'accertamento di identità.

10. INTERAZIONI CON LE AUTORITA'

Il Responsabile del Trattamento coopera con l'Autorità di controllo.
In particolare:

- gestisce le relazioni l'Autorità inerenti alle tematiche di conformità o nell'ambito di indagini conoscitive sull'applicazione del Regolamento, coordinando le attività necessarie per l'evasione delle risposte,
- gestisce gli esposti indirizzati all'Autorità fornendo gli opportuni riscontri all'Autorità stessa e all'interessato.

11. CONCLUSIONI

Pe tutto quanto non previsto nel presente Regolamento interno si rimanda al testo del Regolamento (UE) 2016/679 (General Data Protection Regulation o **GDPR** o Regolamento).