ASSIEME
IN EMILIA ROMAGNA

Uno sguardo sulla normativa delle Associazioni di Promozione Sociale
Servizi di formazione e aggiornamento gratuiti

Tutto in ordine con la privacy?

Martedì 25/2/2025

Relatrice: dott.ssa Francesca Colecchia
Arsea srl

Sommario

Le parole

Il GDPR, trattamento dati personali, dati particolari/dati sensibili, profilazione, misure di sicurezza

I principi

L'accountability, trasparenza e pertinenza, il principio di minimizzazione, la responsabilità

I ruoli

Titolare del trattamento, responsabile trattamento, responsabile della protezione dei dati, responsabile esterno al trattamento dei dati, Amministratore di sistema, incaricato al trattamento dei dati

Le azioni

Informativa, consenso, conferimento incarichi, adozione delle misure di sicurezza, gestione delle violazioni (data breach)

Focus su …

I social, il sito internet, come utilizzare gli strumenti dell'associazione (posta elettronica, mailing list..), l'attività di raccolta fondi e l'utilizzo di fotografie

Le parole

Cosa significa applicare il GDPR?

Il ***General data protection regulation***, è il Regolamento europeo su privacy operativo dal 25 maggio 2018. In qualità di Regolamento ha portata generale per tutti i Paesi membri ed è direttamente applicabile. Alcuni aspetti della privacy sono rimessi alla legislazione degli Stati membri. Il Codice privacy italiano (DLgs 196/2003 modificato dal DLgs 10 agosto 2018, n. 101) rinvia pertanto al GDPR salva l'applicazione di alcune norme che valgono solo nel nostro paese, in particolare si tratta dell'aspetto sanzionatorio.

«La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.»

Cosa significa trattare dati personali?

«**trattamento**»: è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione …

«**dato personale**»: qualsiasi informazione riguardante una **persona fisica** identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Cosa sono i «dati personali particolari»? Quando il trattamento è su larga scala?

Sono dati particolari (sensibili) i dati che rivelino l'origine razziale o etnica, le **opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale,** nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, **dati relativi alla salute** o alla vita sessuale o **all'orientamento sessuale** della persona.

Il giudizio di idoneità all'esercizio dell'attività sportiva agonistica, in quanto dato denotante la normalità psicofisica del soggetto, può ritenersi compreso fra i dati personali "comuni". Al contrario, il referto di inidoneità all'esercizio dell'attività sportiva agonistica, che presuppone nell'interessato la presenza di patologie o, comunque, la necessità di evitare potenziali rischi indotti dalla pratica agonistica, assume invece la connotazione di "dato sensibile", ai sensi dell'art. 22, comma 1 della legge n. 675/1996 (Garante 31 dicembre 1998, in Bollettino n. 6, pag. 111). NB l'associazione conserva i certificati medici ma non i referti che vengono conservati invece dal medico certificatore (Decreto Ministero Salute 8/8/2014).

"*LARGA SCALA*": il numero degli interessati coinvolti, il volume dei dati trattati, la durata delle attività di trattamento o l'estensione geografica del trattamento.
A titolo esemplificativo, il medico di base tratta i dati NON su larga scala ma l'ospedale si Il trattamento su base locale difficilmente è su larga scala mentre un trattamento su base regionale/nazionale/internazionale è più probabile che lo sia.

Cosa si intende per profilazione?

La **profilazione** «*consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona*».

Cosa sono i «BIG DATA»?

Il trattamento automatizzato di grandi quantità di dati acquisiti soprattutto in rete, attraverso i quali, secondo gli analisti ciascuno di noi rischia di essere perfettamente profilato in materia di consumi, abitudini, gusti e opinioni grazie alle tracce digitali che lasciamo in rete e non solo. Tali informazioni si possono desumere dai LIKE sui social, dagli acquisti on line, dai programmi fedeltà nei supermercati, le APP, gli abbonamenti ai servizi streaming, i pagamenti con carta di credito.

Il confine tra DATO PERSONALE e DATO AGGREGATO è sempre più eroso perché oggi – in virtù dei cambiamenti tecnologici – è sempre più semplice partire dal dato aggregato per tornare al dato personale.

Quali cookie possiamo avere?

a) **tecnici:** cookie anonimizzati per garantire la navigazione e la fruizione del sito, non richiedono il consenso;
b) **di profilazione** (volti a creare profili relativi all'utente e utilizzati per inviare messaggi pubblicitari in linea con le preferenze manifestate durante la navigazione): sono cookie non anonimizzati per cui dobbiamo informare gli utenti e ottenere il consenso. Sono disattivi di default;
c) **analitici:** servono a monitorare l'uso del sito da parte degli utenti (ad esempio, quali pagine visitano o qual è la loro provenienza), consentendo perciò di migliorare l'esperienza di navigazione e i servizi offerti dal sito.

Se sono del sito possono essere:

a) anonimi: servono solo a migliorare il sito e sono di default attivi, con possibilità di opposizione;
b) non anonimi perché servono anche a profilare: in questo caso è necessario il consenso e sono non attivi di default.

Se sono di terze parti possono essere:

a) anonimizzati per cui si oscura l'indirizzo IP e la terza parte non può incrociare il dato con altre informazioni ne trasmetterle a terzi;
b) non anonimizzati quando non rispettano le condizioni di cui sopra. E' necessario il consenso e sono non attivi di default.

Quale disciplina per i cookie?

È sempre necessaria l'informativa cookie dai inserire nel footer del sito (può essere aggiuntiva o integrativa dell'informativa privacy generale).
Nell'informativa si elencano i cookie utilizzati/le finalità/il tempo di conservazione dei dati.
Se si utilizzano i cookie di profilazione e quelli analitici non anonimi l'editore del sito deve:

- inserire il banner con info breve sui cookie utilizzati,
- inserire il bottone per accettare/rifiutare/personalizzare l'utilizzo dei cookie,
- inserire il link all'informativa estesa,
- in caso di profilazione, effettuare la valutazione di impatto del trattamento (D.P.I.A. , cioè Data Protection Impact Assesment), un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento,
- informare sui cookie di parte terze le quali dovranno:
    - dare accesso alla informativa tramite link sul sito dell'editore,
    - garantire esecuzione consenso e revoca dei propri cookie,
    - effettuare la DPIA per la propria profilazione.

I principi

Accountability

«L'aver fatto e il poter dimostrare di aver fatto tutto il possibile per evitare il danno».

1) Abbiamo esaminato i rischi connessi al trattamento dei dati per valutare quali misure di sicurezza adottare?

2) Nel fare la valutazione abbiamo preso in considerazioni variabili quali:

- natura dei dati trattati, ossia comuni o particolari/sensibili?
- mole dei dati? Il trattamento avviene su "LARGA SCALA" in considerazione del numero degli interessati coinvolti, del volume dei dati trattati, della durata delle attività di trattamento o l'estensione geografica del trattamento (es: ospedale/trattamento su base regionale/nazionale/internazionale)?

3) Abbiamo riportato in un Documento l'analisi fatta?

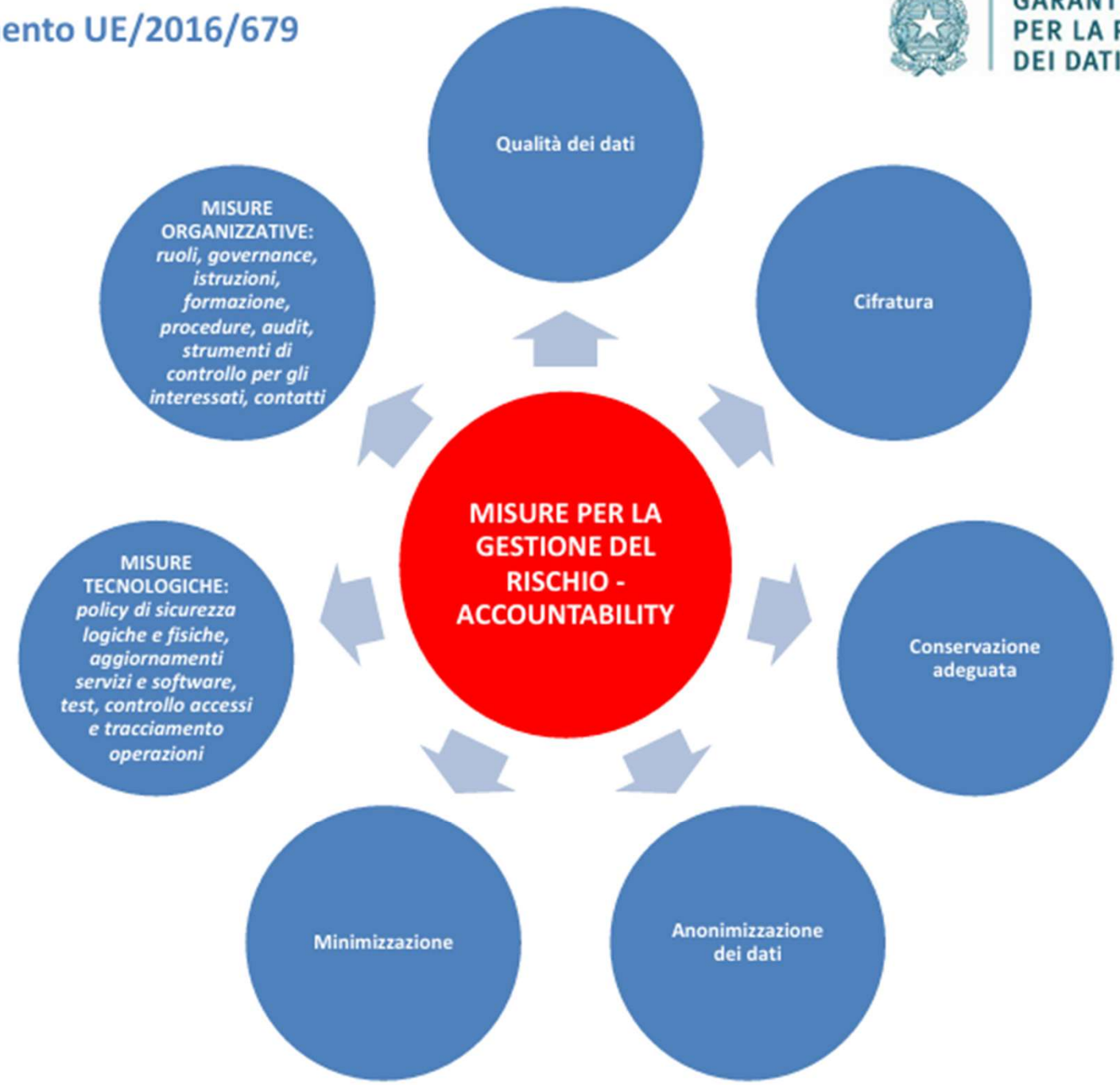
4) Possiamo dimostrare di aver espletato gli adempimenti previsti dal GDPR?

5) Possiamo dimostrare di avere adottato misure di sicurezza coerenti ed idonee rispetto agli scopi?

Accountability

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Trasparenza e pertinenza

L'associazione deve garantire l'assoluta trasparenza gestionale quindi:

a) accessibilità ai verbali;

b) accessibilità al bilancio

ma le modalità di trattamento devono essere pertinenti

Es: in bacheca espongo il cartello in cui invito i soci a versare il contributo annuale entro una determinata data, pena l'esclusione (se lo statuto prevede la morosità come causa di esclusione e quindi sancisce il termine a partire dal quale si configura) ma in bacheca NON espongo il nome dei soci morosi!

Il socio ha diritto di accedere al libro soci?

Si. In tal senso Garante privacy *«ritenuto che il domicilio di ciascun socio, quale risulta registrato nel libro dei soci al momento della richiesta di ispezione, debba essere comunicato al socio che ne faccia richiesta, eventualmente ottenendone "estratti a proprie spese", in occasione dell'esercizio del diritto di ispezione previsto dall'art. 2422 cod. civ. senza che a tal fine sia necessario il consenso del consocio interessato»* (Provvedimento del 26/3/2009 con riferimento alle società)

Trasparenza e pertinenza

«I dati personali riferiti agli associati/aderenti possono essere comunicati agli altri associati/aderenti anche in assenza del consenso degli interessati, a condizione che la predetta comunicazione sia prevista - nell'ambito dell'autonomia privata rimessa a ciascun ente - dall'atto costitutivo o dallo statuto per il perseguimento di scopi determinati e legittimi e che le modalità di utilizzo dei dati siano rese note agli interessati in sede di rilascio dell'informativa ai sensi dell'art. 13 del Regolamento (UE) 2016/679.

In ogni caso, tenendo conto del rispetto dei principi di necessità, finalità e minimizzazione e dell'eventuale regolamentazione interna all'ente, laddove vengano in considerazione profili esclusivamente personali riferiti agli associati/aderenti, devono essere utilizzate forme di consultazione individualizzata con gli stessi, adottando ogni misura opportuna volta a prevenire un'indebita comunicazione di dati personali a soggetti diversi dal destinatario.

La comunicazione dei dati personali relativi agli associati/aderenti all'esterno dell'ente e la loro diffusione possono essere effettuate con il consenso degli interessati, previa informativa agli stessi in ordine alla tipologia di destinatari e alle finalità della trasmissione e purché i dati siano strettamente pertinenti alle finalità ed agli scopi perseguiti.

I dati particolari possono essere comunicati alle autorità competenti per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia» **(Garante privacy provvedimento n. 146 del 5 giugno 2019).**

Il principio di minimizzazione

I dati devono essere «**adeguati, pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati».

Es: un'associazione nel settore socio-sanitario deve valutare l'impatto sociale di una serie di servizi finanziati dall'ASL. Nel questionario saranno richieste una serie di informazioni attinenti ai servizi di cui l'utente ha beneficiato anche in un arco temporale significativo ma l'acquisizione del nominativo di chi compila il modulo non è necessario ai fini della rilevazione.

La responsabilità e le sanzioni

AMMINISTRATIVA	CIVILE	PENALE
Fino a 20 milioni di euro se non ho fornito l'informativo o acquisito il consenso	Risarcimento danni *«Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11»*. (art. 15 DLgs 196/2003) *«Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno»*(art. 2050 c.c.)	❑ Trattamento illecito di dati personali (art. 167 Codice Privacy) ❑ Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala ❑ Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala ❑ Falsità nelle dichiarazioni e notificazioni al Garante ❑ Inosservanza dei provvedimenti del Garante

I ruoli

Le persone

1. Il Titolare del trattamento (*da individuare sempre*)
2. I Responsabili del trattamento
   - il Responsabile (o i responsabili) del trattamento interno/i (*da individuare sempre*)
   - l'amministratore di sistema (consigliato)
   - il Responsabile esterno del trattamento (quando conferisco a terzi il trattamento dei dati – es: commercialista o consulente del lavoro)
3. Il Responsabile della protezione dei dati (obbligatoriamente da individuare nei casi previsti dalla legge)
4. L'incaricato al trattamento dei dati (da individuare sempre)

Il Titolare del trattamento

Il Titolare del trattamento = il Presidente.

È sua la responsabilità in merito alla valutazione del rischio e all'organizzazione di strumenti e procedure idonei a tutelare i diritti delle persone di cui vengono trattati i dati personali e resta in capo al Titolare l'onere di provare di aver adottato misure organizzative e tecniche coerenti con le prescrizioni del Regolamento, anche con riferimento alla verifica del funzionamento delle misure di sicurezza adottate.

Il Responsabile del trattamento

Il o i Responsabili interno/i del trattamento.

È la persona incaricata (con lettera di incarico) dal Titolare del trattamento a:

- ❑ trattare i dati,
- ❑ supervisionare il trattamento dei dati da parte dei soggetti autorizzati;
- ❑ implementare le misure di sicurezza;
- ❑ tenere il Registro dei trattamenti svolti (non obbligatorio sotto i 250 dipendenti ma obbligatorio quando il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di dati "sensibili" o giudiziari;
- ❑ designare il Responsabile della protezione dei dati (RPD-DPO);

in quanto persona che presenti "*garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento*" (81° considerando del GDPR).

L'Amministratore di sistema

Era previsto come obbligatorio quando si trattano dati sensibili a mezzo di strumenti informatici. A lui il compito di ...

- **password**: assegnarle, impostare l'aggiornamento ogni 6 mesi (3 mesi per dati sensibili o giudiziari), conservarle in luogo sicuro e non accessibile a terzi; disattivarle se non utilizzate da almeno sei mesi (a meno che non siano state conferite a chi effettua esclusivamente interventi di gestione tecnica del computer), disattivarle se è venuto meno il conferimento di un incarico al trattamento dei dati (es: perché la persona interessata non collabora più con l'associazione); effettuare, con il responsabile del trattamento dei dati, una verifica periodica dei soggetti autorizzati al trattamento dei dati con strumenti elettronici;
- **backup quotidiano** e adozione di procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- installare ed aggiornare i c.d. **programmi antintrusione;**
- predisporre un **piano di controllo dell'efficacia delle misure di sicurezza** adottate da effettuarsi almeno una volta all'anno.

La prescrizione *«non si applica, invece, a quei soggetti anche di natura associativa che, generalmente dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi»* (precisazioni del Garante - 10 dicembre 2009).

Il Responsabile della protezione dei dati

Il "Responsabile della protezione dati", anche detto RPD o DPO se si utilizza l'acronimo inglese di Data Protection Officer (*NEWS*)

Obbligatorio solo nei seguenti casi:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccetto le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività **principali** del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, **su larga scala**, **di categorie particolari di dati personali** o di dati relativi a condanne penali e a reati.

Il Responsabile della protezione dei dati

L'incarico può essere ricoperto alternativamente da:

a) un dipendente/collaboratore, non in conflitto di interessi;

b) un soggetto esterno;

a condizione che possieda un'approfondita conoscenza della normativa e delle prassi in materia di privacy.

L'assunzione dell'incarico non determina l'assunzione di responsabilità personali in caso di inosservanza del GDPR, spettando al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del GDPR stesso (articolo 24, paragrafo 1 del GDPR).

Qualora non sia nominato il Responsabile della protezione dei dati, tali compiti dovranno essere assolti dal Titolare o dal Responsabile del trattamento.

Il Responsabile della protezione dei dati

I compiti:

a) **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai collaboratori che eseguono il trattamento in merito agli obblighi introdotti dalla normativa;

b) **sorvegliare** l'osservanza della normativa in materia;

c) curare la **sensibilizzazione e la formazione** del personale che partecipa ai trattamenti e alle connesse attività di controllo;

d) fornire, se richiesto e laddove previsto, un **parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento;

e) **cooperare con l'autorità di controllo.**

Il Responsabile esterno al trattamento dei dati

I dati trattati dall'associazione potrebbero essere conferiti a terzi.

Es: società che si occupa delle buste paga dei dipendenti, società che gestisce la piattaforma attraverso la quale vengono effettuate donazioni on line o vengono acquistati servizi da parte di soci o di terzi.

Il Titolare del trattamento dei dati deve pertanto indicare nel contratto sottostante, o in una distinta lettera di incarico, le modalità di trattamento dei dati da parte dei terzi che dovranno assumere l'impegno a:

- trattare i dati nel rispetto del GDPR;
- trattare i dati esclusivamente per gli scopi che realizzare le prestazioni oggetto del contratto;
- collaborare con il Titolare dei dati nella corretta gestione dei dati personali;
- comunicare al Titolare le informazioni relative alle modalità di trattamento e alle misure di sicurezza adottate.

Anche l'associazione può diventare Responsabile esterno del trattamento di dati quando tratta dati di terzi (es: convenzione con la ASL che invia all'associazione gli assistiti).

Quando l'associazione è Responsabile esterno al trattamento dei dati

Es: convenzione con la ASL per un servizio socio-sanitario: i fruitori dei servizi sono inviati dal servizio sanitario o intercettati dall'ente del terzo settore ma sono esterni rispetto all'associazione. I dati personali sono di titolarità del Servizio sanitario che richiede anche il monitoraggio del servizio con indicazione degli accessi ai servizi forniti.

Gli strumenti:

- Conferimento dell'incarico di responsabile esterno al trattamento dei dati;
- La ASL può chiedere all'associazione gli strumenti adottati per tutelare la privacy dei fruitori del servizio;
- A conclusione del progetto i dati devono essere trasferiti alla ASL: si consiglia di trasmetterli come allegato alla rendicontazione del servizio erogato. L'associazione può conservare i dati del progetto anonimizzati.

L'incaricato al trattamento dei dati

Il Titolare o il Responsabile del trattamento dei dati - con l'eventuale supporto del Responsabile della protezione dei dati - dovrà procedere a:

1) autorizzare i collaboratori al trattamento dei dati (adempimento già richiesto dal Codice della privacy) ex art.2 - quardecies DLgs 196/2003;

2) verificare che i collaboratori incaricati al trattamento dei dati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale alla riservatezza (art. 28 GDPR);

3) sensibilizzare e formare gli operatori al tema della privacy, sia con riferimento ai vincoli normativi che con riferimento alle procedure/strumenti adottati internamente per garantire il rispetto del GDPR.

Il conferimento dell'incarico al trattamento dei dati era già previsto dal Codice della Privacy.

Contitorali e Associazioni nazionali

Quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento** quindi determinano, con un accordo interno, le rispettive responsabilità, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni. Indipendentemente da come vengono definiti ruoli e responsabilità dei contitolari, l'interessato potrà in ogni caso esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento. Ciascun titolare dovrà poi espletare gli adempimenti richiesti, in rapporto anche alla natura dei dati trattati, con riferimento alla propria gestione.

Le articolazioni territoriali di un Ente nazionale possono ricevere il conferimento del ruolo di **Responsabili del trattamento** dei dati inerenti al tesseramento e all'affiliazione.

Le azioni

Le azioni

GLI ADEMPIMENTI	LE AZIONI
Informativa	Predisporre l'informativa
Acquisizione del consenso	Adottare il modulo consenso dati
Conferimento degli incarichi	Redigere il verbale del Consiglio Direttivo o specificarlo nelle lettere di incarico
Formazione degli operatori	Seminari
Valutazione del rischio e analisi organizzativa	Riportarla in un verbale del Consiglio Direttivo
Adozione delle misure di sicurezza	Da valutare quali
Redazione e aggiornamento del registro del trattamento dei dati	Da aggiornare con verbale annuale del Consiglio Direttivo
Notifica della violazione della privacy (data breach)	Seguire le indicazioni del GDPR

Privacy: gli elementi dell'informativa

- gli estremi identificativi del titolare e, se designati, del responsabile del trattamento e (*NEWS*) del Responsabile della protezione dei dati personali;
- le finalità e le modalità del trattamento cui sono destinati i dati (art. 13 DLgs 196/2003);
- la natura obbligatoria o facoltativa del conferimento dei dati;
- la base giuridica del trattamento - es: si basa sul consenso espresso dall'interessato (*NEWS*);
- le conseguenze di un eventuale rifiuto di rispondere;
- l'esistenza (*NEWS*) di un processo decisionale automatizzato, compresa la profilazione (*attenzione Google Analytics*);
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- l'intenzione (*NEWS*) del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale (*attenzione Newsletter attraverso programmi*);
- i diritti dell'interessato;
- il periodo di conservazione dei dati o i criteri utilizzati per determinare tale periodo

Informativa: un esempio

INFORMAZIONE PRIVACY (ex art. 13 del Regolamento (UE) 2016/679)

1. Il trattamento dei dati personali conferiti viene effettuato nel rispetto della tutela della riservatezza degli interessati, per gli scopi e nelle modalità di seguito evidenziate. Titolare del trattamento dei dati è _____. Per ogni comunicazione così come per l'esercizio dei diritti riconosciuti all'interessato, è possibile contattare il Titolare via e-mail a _____@_____oppure scrivendo, a mezzo raccomandata, a: _____, Via _____n°__, cap città. Il trattamento dei dati avviene nel rispetto di quanto indicato dalla legge e dalla presente informativa.

2. I dati conferiti sono necessari per:

a) Diventare associati e quindi riceve tutte le informazioni relative alla vita associativa;

b) chiedere - per il tramite della scrivente ___ - il tesseramento alla .... e quindi divenirne soci;

I dati forniti potranno essere comunicati a: ESEMPI

- alla ..... e a Sport e salute nell'espletamento di adempimenti previsti dalla legge e dall'ordinamento sportivo;

Informativa: un esempio

I dati forniti potranno essere comunicati a: ESEMPI

- ai Ministeri ed agli Enti territoriali competenti, nell'espletamento degli adempimenti di legge e/o nella realizzazione di ricerche a fini puramente statistici;

- Nome e cognome dei tesserati potranno essere diffusi, anche attraverso gli organi di stampa, quando contenuti, a titolo esemplificativo, nei verbali di gara e di ogni altra informazione utile al funzionamento delle attività.

- Il conferimento di dati particolari/sensibili può rendersi necessario nell'espletamento degli adempimenti previsti dalla legge *(es: certificato penale per chi opera a diretto contatto di minori)*, dall'ordinamento sportivo (es: *certificato medico di inidoneità all'attività agonistica*), per le particolari esigenze connesse alle attività organizzate (es: *documento attestante allergie per partecipanti a centri estivi)* o per la gestione della pratica assicurativa finalizzata alla liquidazione di un sinistro.

- I dati relativi all'adesione all'associazione devono essere conservati, in ossequio a quanto previsto dal codice civile, per dieci anni. I dati particolari/sensibili saranno trattati per il lasso temporale strettamente necessario in ragione del motivo che ne ha determinato l'acquisizione.

- I dati personali in questione saranno trattati su supporto informatico, magnetico e su supporto cartaceo, da soggetti autorizzati all'assolvimento di tali compiti, costantemente identificati, opportunamente istruiti e resi edotti dei vincoli imposti dalla normativa e che hanno assunto l'obbligo legale alla riservatezza; con l'impiego di misure di sicurezza atte a garantire la riservatezza del soggetto interessato cui i dati si riferiscono e l'indebito accesso a soggetti terzi o a personale non autorizzato.

Informativa: un esempio

- La normativa in materia di privacy (ex art. 7 del DLgs 196/2003 e artt. 12 - 22 del Regolamento (UE) 2016/679) attribuisce alcuni diritti in relazione al trattamento dei dati personali tra i quali:

- il diritto di conoscere, mediante richiesta al Responsabile del trattamento, l'esistenza di trattamento di dati che possono riguardarvi;
- il diritto di ottenere l'aggiornamento, la rettifica ovvero l'integrazione dei dati nonché la loro cancellazione, trasformazione in forma anonima ovvero il loro blocco qualora trattati in violazione della legge nonché il diritto alla portabilità dei dati;
- il diritto di opporsi al trattamento conforme alle finalità sopra indicate solo per motivi legittimi;
- il diritto di opporsi al trattamento dei dati a fini di informazione commerciale o promozionale, di invio di materiale pubblicitario o di compimento di ricerche di mercato;
- il diritto di proporre reclamo all'autorità di controllo http://www.garanteprivacy.it

Informativa: un esempio

PRESTAZIONE DEL CONSENSO DEGLI ASSOCIATI

Per quanto riguarda la prestazione del consenso per il trattamento dei dati effettuato dalla …., si consiglia di utilizzare la seguente dicitura:

Con la presente esprimo il mio consenso al trattamento dei dati personali forniti, nel rispetto di quanto indicato nell'informativa che mi è stata offerta.

Firma ……(per i minori firma del genitore o di chi ne fa le veci)

Presto altresì il consenso alla pubblicazione, in qualsiasi forma, di immagini che mi ritraggono nello svolgimento delle attività organizzate dalla società sportiva dilettantistica, purché la pubblicazione non avvenga per perseguire finalità di natura economica.

Firma ……(per i minori firma del genitore o di chi ne fa le veci)

Privacy: acquisire il consenso

Il consenso può essere espresso verbalmente (no silenzio assenso) ma **meglio per iscritto.** È possibile acquisirlo attraverso moduli, ivi inclusi quelli on line, ma **non possono essere adottate caselle pre-spuntate.** E' obbligatorio acquisirlo per iscritto quando si trattano dati particolari/sensibili.

Nel caso in cui il trattamento dei dati assolva a più funzioni (per esempio l'associazione acquisisce i dati dei soci per la gestione del rapporto associativo ma potrebbe trattare i dati anche per trasmettere comunicazioni commerciali) **è necessario che il consenso sia espresso per ogni singola finalità di trattamento.**

È necessario acquisire un **consenso espresso nel caso di trasferimento dei dati da paesi appartenenti all'UE verso Paesi "terzi"** (non appartenenti all'UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein). Tale specifico consenso non è necessario quando il Paese in questione garantisca un livello di protezione «adeguato» o quando siano previsti strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46). Indicazioni sui Paesi che offrono garanzie e sulle clausole contrattuali idonee a tutelare la privacy sono pubblicate sul sito www.garanteprivacy.it

Privacy: acquisire il consenso

Il consenso è **necessario** fatta eccezione per:

a) esecuzione di un contratto di cui l'interessato è parte;

b) adempiere un obbligo di legge;

c) salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

d) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

e) il perseguimento del legittimo interesse del titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Ho già acquisito il consenso in passato, devo chiederlo nuovamente?

Si solo se non posso provare di averlo acquisito o quando le finalità del trattamento sono cambiate rispetto a quelle originariamente indicate.

Come conferire gli incarichi? La nomina collettiva

Verbale del Consiglio Direttivo

(Omissis) Il Presidente propone di conferire l'incarico al trattamento dei dati i seguenti soci/collaboratori:

1) soci/collaboratori che si occupano esclusivamente del trattamento di dati comuni: sottoscrivendo il presente incarico gli stessi assumono l'obbligo giuridico alla riservatezza ed al rispetto delle prescrizioni in materia di privacy fornite dal titolare e/o dal/i Responsabile/Responsabili del trattamento dei dati:

_____ firma per accettazione _____

_____ firma per accettazione _____

2) soci/collaboratori che si occupano del trattamento di dati comuni e particolati/sensibili: sottoscrivendo il presente incarico gli stessi assumono l'obbligo giuridico alla riservatezza ed al rispetto delle prescrizioni in materia di privacy fornite dal titolare e/o dal/i Responsabile/Responsabili del trattamento dei dati:

_____ firma per accettazione _____

_____ firma per accettazione _____

Il Consiglio Direttivo delibera all'unanimità di procedere in tal senso, dando mandato a _____ di procedere con la richiesta di sottoscrizione del presente verbale per accettazione dell'incarico. Gli incaricati saranno opportunatamente informati delle corrette modalità di gestione degli adempimenti connessi alla tutela della privacy.

(Omissis).

Come effettuo le nomine? Un esempio…

…… nella persona del suo legale rappresentante pro tempore _____ ha deliberato di individuare nella sua persona il Responsabile per il trattamento dei dati personali effettuati dall'associazione.

L'incarico di "Responsabile per il trattamento dei dati personali" comporta l'espletamento delle seguenti attività:

1. procedere al trattamento dei dati personali, attenendosi alle istruzioni impartite dal Titolare, assicurando la puntuale osservanza del pieno rispetto delle vigenti disposizioni in materia;
2. curare che l'eventuale personale incaricato al trattamento operi in conformità alle disposizioni di legge e regolamentari impartite a tale proposito;
3. avere cura che ogni dato, elenco o banca dati cartacea, informatica e telematica venga trattato per i soli fini per i quali è destinato;
4. controllare che i dati personali vengano comunicati e/o diffusi nel rispetto delle prescrizioni che Le saranno impartite;
5. verificare che sia effettuata l'informativa privacy;
6. controllare che gli incaricati raccolgano il consenso scritto dell'interessato per il trattamento dei dati personali e per la loro comunicazione e diffusione, se necessarie;
7. controllare che i dati personali vengano trattati nel rispetto delle modalità di raccolta e trattamento specificati nell'informativa privacy;

Come effettuo le nomine? Un esempio...

8. autorizzare di volta in volta la comunicazione e/o la diffusione dei dati personali;
9. conservare i dati personali raccolti su supporti cartacei ed i dati personali raccolti su supporti informatici nel rispetto delle misure di sicurezza adottate, osservando in particolare i seguenti requisiti minimi di sicurezza:
- attribuzione di password per l'accesso ai sistemi informatizzati utilizzabili solo dagli incaricati;
- custodia delle pratiche che contengono dati personali, soprattutto se "sensibili", in armadi o cassetti chiusi a chiave dopo l'uso;

(altre indicazioni di sicurezza)

Con preghiera di sottoscrivere la presente a titolo di ricevuta e per accettazione integrale del suo contenuto, Le porgiamo distinti saluti.

Le misure di sicurezza

Le **misure di sicurezza** possono consistere (Considerando 78, 79 del GDPR) in:

1) ridurre al minimo il trattamento dei dati personali;

2) garantire trasparenza per quanto riguarda le funzioni ed il trattamento dei dati personali;

3) ripartire in modo chiaro le responsabilità nel trattamento;

4) **adottare le misure tecnologiche adeguate** ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (es: la **pseudonimizzazione** e la **crittografia** dei dati personali).

La **valutazione del rischio**: *"la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato"* (76° Considerando del GDPR).

Le misure di sicurezza

Crittografia e pseudonomizzazione hanno l'obiettivo di **oscurare i dati per renderli illeggibili** da coloro che non hanno la chiave per accedervi.
La **crittografia** è basata su un algoritmo che oscura i dati e su una "passphrase" che apre o chiude la visualizzazione.
La **pseudonomizzazione**, invece, fa in modo che i dati acquisiti o trattati non siano riconducibili ad una persona fisica identificata o identificabile.

Non sapete quali misure di sicurezza adottare per i dati trattati attraverso strumenti informatici?
L'amministratore di sistema è la figura che dovrebbe supportarvi in questo!

Le misure di sicurezza

Qualora i trattamenti "*possano presentare un* ***rischio elevato*** *per i diritti e le libertà delle persone fisiche*" si rende necessario effettuare una "***valutazione d'impatto sulla protezione dei dati*** (DPIA) *per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio*" al fine di individuare opportune misure per dimostrare che il trattamento dei dati personali rispetta il Regolamento (84° considerando del GDPR).

La valutazione d'impatto dovrebbe essere effettuata in particolare con riferimento ai «*trattamenti su larga scala*» o nei casi di profilazione dei dati.

La DPIA consente di analizzare sistematicamente e approfonditamente come un nuovo trattamento, una nuova tecnologia, o un nuovo progetto (oppure la modificazione sostanziale di un trattamento in corso o delle finalità o delle metodologie tecnologiche preesistenti) impatteranno sui diritti e le libertà degli interessati ed individuare quali misure implementare per la tutela di quest'ultimi – approccio definito ***privacy by design & by default.***

Quando è necessario fare la valutazione di impatto sulla protezione dati?

PRINCIPIO: *la valutazione si effettua quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto (trattamento effettuato su larga scala) e le finalità del trattamento (o implichi la profilazione), può presentare* ***un rischio elevato per i diritti e le libertà delle persone fisiche***

e si tratti di trattamenti

- non occasionali di soggetti vulnerabili (*minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo*);
- di categorie particolari di dati interconnessi con altri dati personali raccolti per finalità diverse;
- trattamenti sistematici di dati biometrici, tenendo conto del volume dei dati, durata, persistenza;

+ altre categorie che non interessano il Terzo settore come chi effettua lo screening sui clienti di una banca attraverso l'utilizzo dei dati registrati in una centrale rischi, chi effettua trattamenti in ambito telecomunicazioni, banche per l'offerta di servizi antifrode, antispam, sicurezza; chi effettua la geolocalizzazione, chi effettua la videosorveglianza dei dipendenti.

Elenco completo su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979

Quando la DPIA è obbligatoria?

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento). **La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.**

Chi effettua la DPIA? In quale momento?

La responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione.

Il titolare ne monitora lo svolgimento consultandosi con il responsabile della protezione dei dati (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer, CISO) e del responsabile IT.

La DPIA deve essere condotta prima di procedere al trattamento. Dovrebbe comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari.

Il Registro del trattamento dei dati (art. 30 GDPR)

Non obbligatorio per chi ha meno di 250 dipendenti, a meno che

- il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato,
- il trattamento non sia occasionale o
- il trattamento **includa dati particolari**, ivi inclusi quelli **relativi a condanne penali.**

Adempimento simile al Documento programmatico sulla sicurezza (DPS) che doveva essere redatto da quanti trattavano dati sensibili attraverso il computer (art. 34 del DLgs 196/2003 + punto n. 19 dell'Allegato B) al DLgs).

Per effettuare una **valutazione del rischio**, è possibile ricorrere alla guida operativa per redigere il DPS (orientativa e non vincolante) elaborata dal Garante privacy, consultabile su

http://www.privacy.it/archivio/garanteprovv20040611.html

Il Registro del trattamento dei dati (art. 30 GDPR)

chi siamo	
come è possibile contattare il titolare/contitolare/responsabile della protezione dei dati?	
perché trattiamo i dati	
quali dati trattiamo? Ci sono diverse categorie di interessati ?	
a chi possiamo comunicare i dati? Li comunichiamo anche ad organizzazioni internazionali, ad organizzazioni con sede fuori dall'Europa?	
quando procediamo alla cancellazione dei dati?	
quali sono i rischi nel trattamento dei dati e quali sono le misure di sicurezza tecniche e organizzative adottate?	

Notificare la violazione dei dati *(data breach)*

Abbiamo perso la chiavetta all'interno della quale avevamo l'anagrafica dei soci?

Abbiamo perso il faldone con i certificati medici degli atleti della nostra associazione sportiva?

Queste sono violazione della tutela della privacy!

Cosa dobbiamo fare?

1) dobbiamo documentare questa violazione (lo scriveremo in un verbale del Consiglio Direttivo o lo inseriremo nel Registro del trattamento dei dati) ed indicare i provvedimenti adottati;
2) se l'associazione scopre una violazione dei dati personali qualora si ritenga che da tale violazione possano derivare rischi per i diritti e per le libertà degli interessati dovrà comunicarlo all'Autorità di controllo entro 72 ore e se il rischio per gli interessati si ritiene elevato, è necessario informare anche loro della violazione.

Focus su ...

Trattare dati attraverso il SITO/Newsletter/APP

È necessario acquisire informazioni da chi gestisce l'applicazione con particolare riferimento ai seguenti aspetti:

1) vengono utilizzati *(direttamente o indirettamente)* solo cookie (*sono piccoli file di testo che i siti visitati inviano al terminale che l'utente utilizza per accedere al sito, il terminale li memorizza e li ritrasmette al sito alla visita successiva*) tecnici o anche cookie o altri strumenti di profilazione (*per esempio effettuano la profilazione Google Analytics, Youtube, Facebook: se vengono utilizzati attraverso l'applicativo è necessario specificare nell'informativa che il trattamento dei dati prevede la profilazione e rinviare alla privacy policy del soggetto che realizza la profilazione*);

2) vengono trasmessi i dati in paesi extra europei? La vostra associazione potrebbe non trasferirli in maniera consapevole ma potreste avvalervi di strumenti per l'invio di Newsletter gestiti da società extra europee (es: MailChimp ha sede negli USA) ed è un aspetto da indicare in INFORMATIVA.

«Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.» (art. 3 GDPR)

Quando apri la pagina FACE BOOK …

- stipuli un contratto che prevede l'adesione alle condizioni di utilizzo della pagina FB, inclusa la politica ad essa relativa in materia di cookie;
- Facebook posiziona sul computer/smartphone delle persone che hanno visitato la PAGINA (a prescindere dalla circostanza che abbiano un profilo FB), cookie per memorizzare informazioni nei browser web che, se non eliminati, restano attivi per 2 anni. Facebook riceve, registra ed elabora le informazioni memorizzate nei cookie così come possono farlo i partner di Facebook;
- l'amministratore di una PAGINA FACEBOOK contribuisce al trattamento dei dati e può tramite filtri messi a disposizione da Facebook, definire i criteri a partire dai quali si devono stabilire tali statistiche (geolocalizzazione, età, sesso, situazione sentimentale e professionale, informazioni sugli interessi, le categorie di prodotti o di servizi di loro maggiore interesse) e designare perfino le categorie di persone i cui dati personali saranno oggetto di utilizzo da parte di Facebook.

… diventi responsabile del trattamento effettuato anche da Facebook (Corte di Giustizia UE, sentenza 5/6/2018, causa C-210/16): devi quindi informare gli utenti che FB - attraverso *cookie* attivati sul disco rigido - tratta i relativi dati per realizzare statistiche sugli utenti destinate al gestore di detta pagina e permettere a FB di diffondere pubblicità mirate.

Quando fai attività di raccolta fondi …

PRINCIPIO GENERALE: *«nei confronti del donatore e del beneficiario dovrà essere garantito il rispetto della privacy, soprattutto in ordine al trattamento dei dati personali secondo quanto previsto dall'articolo 13 del d. lgs. n. 196/2003, e dal Regolamento europeo sulla Privacy, GDPR 2016/679»* ***(Linee guida raccolta fondi).***

RACCOLTA FONDI ATTRAVERSO IL DIRECT MAIL, **ossia** qualsiasi tipo di comunicazione diffuso per via postale. Le organizzazioni devono assicurarsi che le banche dati di cui si servono per la spedizione siano aggiornate in modo da includere solo le persone che abbiano fornito in precedenza consenso espresso e specifico all'invio di materiale informativo e non lo abbiano revocato successivamente. **Nella comunicazione deve essere fatto espresso richiamo alla normativa sulla privacy e devono essere indicate le finalità della raccolta, gli strumenti attraverso i quali effettuare le donazioni, con indicazione dei benefici fiscali, gli indirizzi dell'organizzazione da contattare per ricevere informazioni ulteriori** *(Linee guida raccolta fondi).*

Quando fai attività di raccolta fondi ...

RACCOLTA FONDI ATTRAVERSO NUMERAZIONI SOLIDALI

Si tratta di una modalità di raccolta fondi che prevede un contratto tra organizzazione non profit e gestore del servizio (*ossia soggetti aderenti al Codice autorizzati a fornire al pubblico servizi di comunicazioni elettronica in grado di gestire numerazioni 455XY*) in virtù del quale il gestore ha un mandato con rappresentanza, ex art. 1704 del cod. civ., per riscuote la donazione effettuata sia attraverso SMS sia da utenze di telefonia fissa attraverso una chiamata in fonia e che prevede l'integrale devoluzione di quanto ricevuto all'Organizzazione senza scopo di lucro. Per gestire questo contratto il 2/2/2018 l'AGCOM ha adottato il «codice di autoregolamentazione per la gestione delle numerazioni utilizzate per le raccolte fondi telefoniche per fini benefici di utilità sociale» consultabile qui https://www.agcom.it/. Tale servizio è esente IVA per le organizzazioni destinatarie della numerazione (Legge 28 febbraio 2005, n.21)

Gli operatori telefonici potranno comunicare agli enti no-profit i dati di quanti hanno donato fondi attraverso sms o telefonate da rete fissa, verso la numerazione con codice "455", per permettere agli enti di rendicontare ai donatori i risultati delle iniziative cui hanno aderito. Gli enti potranno ricontattare i donatori per promuovere nuove campagne di fundraising solo nel caso in cui questi ultimi abbiano espresso il loro consenso. Il Garante ha chiarito, inoltre, che nell'informativa dei gestori telefonici e degli enti no-profit dovranno essere specificati, già in forma sintetica al momento della donazione (con rinvio ad un'informativa più estesa reperibile sui relativi siti di riferimento), il ruolo di contitolarità dei diversi attori e le differenti finalità di trattamento. Società telefoniche ed enti no-profit dovranno infine mettere a punto un sistema che agevoli l'esercizio dei diritti del donatore: in particolare, quello di revoca del consenso, che, come prevede il Regolamento Ue, deve poter essere esercitato "con la stessa facilità con cui è stato accordato" (Garante privacy Newsletter n. 446 del 15/11/2018).

Quando fai … telemarketing …

RACCOLTA FONDI ATTRAVERSO IL TELEFONO (TELEMARKETING). Il telemarketing può svolgersi con modalità inbound, cioè ricevendo le chiamate presso l'organizzazione/call center che opera per conto della stessa. L'altra modalità, detta outbound, consiste nell'effettuazione di telefonate da parte dell'organizzazione/call center a donatori, soci, simpatizzanti i cui nominativi sono presenti nella banca dati dell'organizzazione, a tutti coloro **che comunque abbiano fornito consenso al trattamento dei propri dati personali.** Vincoli: rendere visibile il numero telefonico del chiamante; comunicare con chiarezza le generalità dell'operatore e dell'ente; informare sullo scopo della telefonata e delle modalità di effettuazione delle donazioni, sugli importi richiesti ed i benefici fiscali collegati, sui recapiti dell'Ente con indicazione del referente della raccolta al quale chiedere informazioni e tutte le informazioni richieste dalla normativa privacy.

Se l'utente dice "no" alla telefonata commerciale indesiderata il call center o la società che lo ha contattato deve annotare subito la sua volontà e cancellare il nominativo dalle liste utilizzate per il telemarketing. L'opposizione espressa nel corso della telefonata non deve essere confermata con email o altre modalità, come invece viene spesso richiesto di fare da parte degli operatori, ed è valida anche per le campagne promozionali future. Il principio è stato affermato dal Garante privacy che, al termine di una complessa attività istruttoria, ha rilevato diverse condotte illecite messe in atto da Edison Energia spa nei confronti di un numero rilevante di utenti. L'Autorità ha quindi ingiunto alla società l'adozione di una serie di misure per mettersi in regola e le ha ordinato il pagamento di una sanzione di 4 milioni e 900 mila euro. L'atto è consultabile qui: https://www.garanteprivacy.it/.../docweb.../docweb/9856345

Quando fai fotografie ...

L. 633/1941 (Legge sul diritto d'autore)

Art. 96 - *Il ritratto di una persona* ***non può essere esposto, riprodotto o messo in commercio senza il consenso*** *di questa, salve le disposizioni dell'articolo seguente.*

Art. 97 - ***Non occorre il consenso*** *della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata.*

Attenzione ai minori!

Secondo la Cassazione, laddove non si riscontri alcuna utilità sociale della notizia, nel bilanciamento degli opposti valori costituzionali, e quindi del diritto di cronaca e del diritto alla privacy, la riservatezza del minore è da considerarsi assolutamente preminente.

artt. 2 e 31 della Costituzione e Convenzione internazionale sui diritti dell'infanzia del 20/11/1989, ratificata con legge n. 176/1991.

Quando fai fotografie ...

La foto è un dato personale?

Si in quanto informazione idonea a consentire l'identificazione di un soggetto (Garante 2 luglio 1997).

La foto è un dato particolare?

Le informazioni estrapolabili dalla foto devono essere considerate "comuni" **a meno che dalle immagini non possano ricavarsi elementi che rimandino, anche in modo indiretto, alla categoria dei c.d. «dati sensibili»** (Garante 26 marzo 2003)

La foto non viene considerato dato biometrico di per sé (servono degli applicativi per estrarre informazioni biometriche) ma dal contesto potrebbero emergere dati particolari/sensibili (es: partecipazione ad una celebrazione religiosa, ad un comizio politico, ad una manifestazione sindacale).

Le fotografie nell'ambito di un progetto: un esempio

DENOMINAZIONE INIZIATIVA/PROGETTO REALIZZATO DA _____

Il/la sottoscritto/a .....(cognome e nome) nato/a a..... il.....residente a..... prov. ..... cap.....in via/piazza..... n°..... tel. .....e-mail..... C.F. ..... nella qualità di genitore del/della minore ..... (cognome e nome) nato/a ..... il ..... residente a ..... prov. ..... cap. ..... in via/piazza ..... tel. fisso ..... tel. cellulare .... e-mail ..... cod. fiscale .....

CHIEDE L'ISCRIZIONE

Alle attività connesse al progetto "....." che si terranno dal _____ al _____, dichiarando di aver preso visione del programma delle attività_____,

DATA - FIRMA (se minore anche del genitore o di chi ne fa le veci)

CONSENSO AL TRATTAMENTO DI DATI PERSONALI.

Con la presente dichiaro di aver ricevuto l'informativa sui diritti connessi al trattamento dei dati personali miei [e del/della minore che rappresento] da parte dell'associazione ....., trattamento finalizzato alla realizzazione delle attività promosse dall'associazione e all'adempimento di ogni obbligo di legge, ivi inclusa la rendicontazione dell'attività. Presto, pertanto, il consenso al trattamento dei dati per le finalità sopra descritte ai sensi della normativa in materia di privacy (Regolamento Europeo sulla privacy 2016/679 -GDPR e DLgs 196/2013).

DATA - FIRMA (se minore anche del genitore o di chi ne fa le veci)

Le fotografie nell'ambito di un progetto: un esempio

AUTORIZZAZIONE ALL'UTILIZZO DELL'IMMAGINE.

Con la presente esprimo inoltre il mio consenso alla pubblicazione, in qualsiasi forma, di immagini che ritraggono il/la minore rappresentato/a nello svolgimento delle iniziative del progetto, purché la pubblicazione non abbia come scopo il relativo sfruttamento commerciale e non violi il decoro della persona ritratta. Le immagini potranno essere veicolate attraverso qualsiasi strumento (come, a titolo esemplificativo e non esaustivo, pubblicazione sul sito internet, sui social network, attraverso Newsletter) e potranno essere veicolate da ..... nonché da terzi, quali gli organi di stampa e gli enti finanziatori del progetto.

DATA - FIRMA (se minore anche del genitore o di chi ne fa le veci)

La check-list

L'informativa che utilizziamo contempla tutti i requisiti richiesti?	Slide 32
Abbiamo acquisito il consenso degli interessati al trattamento dei dati? Come? Possiamo provarlo?	Slide 37
Abbiamo conferito gli incarichi?	Slide 39
Abbiamo informato responsabili/incaricati su come gestire la privacy?	Specificarlo in un verbale
Ci siamo preoccupati della privacy anche rispetto al sito internet ed ai social?	Attenzione all'informativa
Abbiamo valutato le misure di sicurezza da adottare in rapporto anche alla tipologia e mole di dati trattati?	Specificarlo in un verbale