IL TRATTAMENTO DEI DATI PERSONALI NELLE ASSOCIAZIONI DI VOLONTARIATO E NEGLI ENTI DEL TERZO SETTORE

EDIZIONE 2020
Avv. Davide Cester

PRESENTAZIONE ALLA TERZA EDIZIONE

Quando nel lontano 1997 è entrata in vigore la prima legge italiana sul trattamento dei dati personali (L. n. 675/1996), la privacy si è introdotta nelle cassette della posta degli italiani attraverso burocratiche informative e richieste di consenso per i più disparati trattamenti di dati.
Poi, nel 2003 è entrato in vigore il Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003).
Ma sembra già preistoria, se si pensa che nel 2017 una società inglese sembra aver influenzato le elezioni americane attraverso l'acquisizione e la profilazione dei dati degli utenti di Facebook.
E che ormai la "vecchia" privacy inglese – il diritto ad "essere lasciati soli" – non esiste più, perché ogni giorno noi stessi invitiamo a "casa nostra", attraverso le frequentazioni informatiche, i social network, le chat, innumerevoli persone, enti e società.
In piena era digitale, il nuovo Regolamento UE 2016/679 ("GDPR") – da applicarsi dal 25 maggio 2018 – si propone di fissare regole e diritti comuni in ambito europeo, che anche i colossi web mondiali devono rispettare se utilizzano dati di cittadini europei.
Si devono spaventare le associazioni ed in generale gli enti del Terzo Settore, magari di piccole dimensioni e di ristretta attività?
Innanzitutto, il Regolamento si pone comunque in linea con il "vecchio" Codice Italiano, e quindi un trattamento dei dati conforme alla normativa del 2003 risulta già soddisfare molte previsioni del GDPR.
Chi è stato attento alla privacy fino ad ora avrà meno difficoltà ad aggiornarsi.
Quello che certamente non aiuta è la previsione di incombenze, oneri e sanzioni (anche di grande entità) teoricamente applicabili anche alle piccole realtà profit e non profit, e questo trattamento molto spesso "indifferenziato" tra grandi e piccoli discende anche dal fatto che la dimensione del Titolare del trattamento non sempre costituisce un indice direttamente proporzionale alla pericolosità o rilevanza del trattamento dei dati svolto (infatti, per comunicare o utilizzare innumerevoli dati può bastare anche un solo computer e una singola persona).
Aggiungasi che il quadro normativo e regolamentare risulta costantemente in evoluzione: il legislatore italiano ha adottato il Decreto Legislativo attuativo del GDPR (D.Lgs. n. 101/2018, che è intervenuto a modificare proprio il "vecchio" Codice di cui al D.Lgs. n. 196/2003, rimasto quindi in vigore), ma per vari settori e aspetti si attendono i provvedimenti del Garante, i pareri del Comitato Europeo, ecc. e altro ancora.
In quest'ottica, risulta fondamentale anche per le Associazioni di Volontariato e gli Enti del Terzo Settore la conoscenza del proprio sistema di trattamento dati, l'individuazione dei rischi maggiori soprattutto in relazione ai trattamenti di dati particolarmente delicati (i vecchi "dati sensibili") e l'individuazione di una politica della privacy estesa a tutti i membri.
Il Regolamento stabilisce espressamente il proprio scopo nel garantire che il trattamento dei dati sia "al servizio della persona", e si tratta allora di un fine che il Terzo Settore conosce bene.
Anche nel mondo del volontariato e del Terzo Settore continua quindi ad esserci ampio spazio per quella che è stata confermato e continua ad essere uno dei presupposti della privacy: uno stile di servizio basato sul rispetto della persona, sull'attenzione e sulla fiducia, sulla capacità di accostarsi e di capire che tipo di "vicinanza" instaurare, e soprattutto di rendere certa la persona che il rapporto con l'ente sarà "fiduciario" e quello con il volontario o il socio confidenziale ed esclusivo.

PRESENTAZIONE ALL'AGGIORNAMENTO DELL'APRILE 2020

Rispetto alla terza edizione sono state aggiornate alcune D/R sulla base dei sopravvenuti provvedimenti del Garante per la protezione dei dati personali, sono stati introdotti alcuni modelli nuovi e resi più funzionali alcuni modelli già presenti, e si è aggiunta una nuova D/R dedicata al trattamento delle immagini/video.

Davide Cester, avvocato Cassazionista in Padova, è consulente legale del Centro di Servizio per il Volontariato della Provincia di Padova dal 2003 e collabora altresì con i Centri di Servizio Sardegna Solidale, di Verona, Treviso, Vicenza e Rovigo. Ha già pubblicato per il mondo del terzo settore, "La privacy nelle associazioni di volontariato e non profit" (Elementi, 2009). Svolge l'incarico di Data Protection Officer (DPO) in pubbliche amministrazioni ed è consulente legale di Enti del Terzo Settore.

IMPORTANTE – ISTRUZIONI PER L'USO

Il tentativo di rendere chiare e immediatamente applicabili le norme del nuovo Regolamento UE 2016/679 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" e di spiegarne l'effettiva portata in ambito di volontariato e *non profit* cela sicuramente dei rischi non indifferenti.
La normativa europea è infatti complessa ed estesa e la sua corretta applicazione può e deve variare da caso a caso, a seconda delle caratteristiche della singola Associazione che tratta dati personali e del tipo di trattamento di dati effettuato.
Le norme generali possono poi essere derogate da regole specifiche relative a settori determinati, come ad esempio l'ambito sanitario, o giudiziario, o pubblico, o relativo ai rapporti di lavoro, la cui approfondita analisi necessariamente esula dal contenuto di questo lavoro.
Le risposte, i commenti e gli esempi riportati costituiscono quindi dei criteri di massima e vanno sempre valutati con riferimento alla propria realtà associativa e al progressivo evolversi delle fonti giuridiche.
Il presente lavoro è disponibile in forma di FAQ o quale pubblicazione on line nei siti istituzionali dei Centri di Servizio per il Volontariato di Padova, Verona, Treviso, Rovigo e Sardegna Solidale, ove si potranno reperire i successivi aggiornamenti.

ATTENZIONE

DOMANDE E RISPOSTE: I QUESITI PIÙ IMPORTANTI

Si riportano qui di seguito 30 domande/risposte su contenuto e prescrizioni del Regolamento UE 2016/679 e sulle ricadute concrete della disciplina per le Associazioni di Volontariato (ODV) e di Promozione Sociale (APS) e in generale per gli Enti del Terzo Settore (ETS).

1. Cosa è cambiato con il Regolamento Europeo? Esiste ancora la "vecchia" privacy?

Il Regolamento UE del Parlamento e del Consiglio Europeo 2016/679 detto "**General Data Protection Regulation**" (in breve "**GDPR**", pronunciato in inglese "GiDiPiAr"), entrato in vigore in data 25.5.2018, segna una ulteriore accelerazione nel campo della tutela della riservatezza e del trattamento dei dati personali.

Con la definitiva esplosione dei social network, delle piattaforme informatiche, delle App e dei motori di ricerca, le persone fisiche si comportano spesso in modo sostanzialmente opposto alla propria riservatezza, rendendo disponibili ai propri amici, al pubblico, alle imprese e alle autorità pubbliche, su scala europea e mondiale, innumerevoli informazioni personali.

La libera circolazione dei dati favorisce gli scambi, le relazioni sociali, la conoscenza, il confronto, ma cela anche vari rischi. Il Regolamento lo dice chiaramente: il trattamento dei dati deve essere "*al servizio dell'uomo*", che non deve esserne schiavo o oggetto. Perché questo accada ogni persona deve essere posta in grado di avere il controllo su come i suoi dati, singoli o organizzati, vengono utilizzati, nell'ambito di un quadro europeo (e internazionale) di regole comuni.

Il testo del Regolamento è riportato nelle pagine finali di questo lavoro ed è disponibile nel sito del Garante per la Protezione dei Dati Personali ***www.garanteprivacy.it*.**

Il GDPR non ha comportato l'abrogazione della "vecchia" normativa italiana ("Codice in materia di protezione dei dati personali" di cui al D.Lgs. n. 196/2003). Infatti, il governo italiano, con **D.Lgs. n. 101 del 10.8.2018**, è intervenuto sul vecchio Codice del 2003 abrogandone solo gli articoli riguardanti aspetti disciplinati direttamente dal GDPR, ma mantenendo e aggiornando quelle parti che riguardano aspetti di dettaglio sui quali il GDPR ha consentito agli Stati membri di legiferare.

2. Definizioni vecchie e nuove

Per comprendere il GDPR è necessario avere un minimo di familiarità con i seguenti concetti/definizioni contenuti nell'art. 4, che non si differenziano peraltro in termini rilevanti rispetto a quelli del Codice italiano del 2003.

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 è "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), e quindi il nome, la foto, l'indirizzo mail, le coordinate bancarie, i post nei social network, i referti medici, un provvedimento giudiziale, ecc.

INTERESSATO è la persona fisica identificata o identificabile attraverso i suoi dati personali. "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". Non è soggetto "interessato", per il GDPR, la persona giuridica.

TITOLARE ("**data controller**") è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

RESPONSABILE DEL TRATTAMENTO ("**data processor**") è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

PROFILAZIONE è "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

PSEUDONIMIZZAZIONE è "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

Nonostante il Regolamento non riproponga alcune definizioni del Codice, restano comunque valide altre definizioni quali:

INCARICATI/AUTORIZZATI: le persone fisiche autorizzate dal Titolare o dal Responsabile a compiere operazioni di trattamento

COMUNICAZIONE DEI DATI: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato [...], dal responsabile e dagli incaricati/autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

DIFFUSIONE DEI DATI: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

3. Qual è lo scopo del GDPR?

Il GDPR vuole garantire che il trattamento dei dati personali dei cittadini dell'Unione Europea, e cioè l'utilizzo delle informazioni e notizie che li riguardano, si svolga nel rispetto dei diritti e delle libertà fondamentali, con particolare riferimento al diritto alla protezione dei dati personali (art. 1).

Più precisamente, il GDPR, in termini non molto diversi dal Codice italiano (D.Lgs. n. 196/2003), si propone soprattutto di far sì che i dati personali delle persone fisiche:

a) vengano utilizzati per **scopi leciti** e comunque per le **finalità** in base alle quali sono stati raccolti e non oltre il tempo necessario per raggiungere tali finalità;
b) **non siano conosciuti da estranei non autorizzati** e che non vengano diffusi o comunque utilizzati contro la volontà o nell'ignoranza della persona cui si riferiscono;
c) non vengano distrutti o perduti.

4. Quali dati trattano le Associazioni e gli Enti del Terzo Settore e che natura hanno?

Le Associazioni e in genere gli ETS raccolgono e utilizzano comunemente, nello svolgimento della loro attività istituzionale, dati personali

a) dei propri **soci**/aderenti/volontari
b) dei **beneficiari** dell'attività istituzionale o degli utenti del servizio
c) dei ragazzi in servizio civile e dei volontari di giustizia riparativa
d) dei consulenti, **collaboratori** esterni e dei fornitori
e) degli eventuali **dipendenti** o lavoratori autonomi
f) dei **partecipanti** ad eventi organizzati dall'ETS
g) degli utenti del **sito** istituzionale
h) degli iscritti alla **newsletter**
i) degli enti pubblici e degli altri ETS
j) dei donatori
k) delle persone, enti e aziende a cui indirizzare campagne di sensibilizzazione e *fundraising*.

*Costituiscono per esempio **raccolte cartacee** di dati personali il libro dei soci, il libro dei volontari, la rubrica per la corrispondenza, l'elenco dei donatori, ecc. Tali dati in vari casi sono però gestiti **in via informatica** e sono contenuti in **banche dati**, in alcuni casi anche mediante sistemi di cloud, situazioni che richiedono l'adozione di particolari misure di sicurezza e di protezione.*

Quanto alla natura dei dati, permane la distinzione tra:

→ **DATI COMUNI** (es. il nominativo, la data di nascita, il numero di cellulare dei soci/volontari o beneficiari, l'indirizzo mail, l'avvenuto versamento della quota associativa, gli studi compiuti)
→ **DATI SENSIBILI**, che il GDPR chiama "**PARTICOLARI CATEGORIE DI DATI**"
→ **DATI GIUDIZIARI**

Costituiscono dati personali ~~(comuni o sensibili)~~ anche le **IMMAGINI**, i suoni, i video ecc., quando consentono di individuare la persona a cui si riferiscono. Anche a tali dati, quindi si applicano le regole del GDPR, oltre alle norme civilistiche sulla tutela dell'immagine (vedi D/R n. 30).

Non sono invece soggetti a tutela, ai sensi del GDPR, i **dati delle persone giuridiche**, ma solo quelli delle persone fisiche che ne fanno parte.

5. Il GDPR riguarda anche le Associazioni e gli ETS? Si devono considerare "Titolari del trattamento"? Possono essere "Contitolari del trattamento"?

Assolutamente SI, buona parte delle norme del GDPR si applicano anche alle Associazioni ed in generale agli Enti del Terzo Settore, che sono "**Titolari** del trattamento" se e ogni qualvolta svolgono al loro interno anche una sola delle operazioni che concretano un trattamento di dati personali, decidendo la finalità e le modalità del trattamento stesso.

Restano esclusi dall'applicazione del GDPR i trattamenti di dati svolti da "una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico" (es. rubrica telefonica nella propria abitazione, impianto di sorveglianza ad uso esclusivamente privato, ecc.) e sempre che non si svolga una comunicazione sistematica o diffusione. Il trattamento di dati svolto da un ETS non ha fini esclusivamente personali, comporta molte volte una comunicazione a terzi, e rientra pertanto nell'ambito di applicazione delle norme del GDPR, ed in particolare ***di tutte le norme applicabili agli enti privati****, quali sono le Associazioni, le Fondazioni, le Cooperative Sociali, ecc. Non c'è quindi una sostanziale differenza tra un ETS e una società commerciale in relazione all'applicazione delle norme del GDPR, salvo in relazione alle poche norme del GDPR espressamente riferite a "fondazioni, associazioni o organismi senza scopo di lucro" (principalmente, l'art. 9, comma 2 lett. d del GDPR sulla legittimità del trattamento dei dati sensibili dei soci/aderenti). In questa categoria generale (e generica) indicata dal GDPR rientrano probabilmente anche le associazioni e organismi no profit che non sono iscritti al registro del volontariato ex L. 266/91 o al registro della promozione sociale ex L. 383/00 o non saranno iscritti al RUNTS di prossima costituzione in base al Codice del Terzo Settore; sembrano rientrare secondo il Garante anche le Cooperative Sociali e le Imprese Sociali (che sono certamente ETS ai sensi dell'art. 4 D.Lgs. n. 117/2017, ma perseguono un profitto con finalità mutualistica), posto che il Garante le ha parificate agli altri ETS nel provvedimento/autorizzazione generale del 5.6.2019 riferito proprio al "trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose".*

Titolare del trattamento è la persona giuridica nel suo complesso (e quindi l'Associazione, la Fondazione, il Comitato, ecc.) **e non le persone fisiche che ne fanno parte o che ne hanno la rappresentanza legale**.

Ciò non toglie:

- che le decisioni sui trattamenti da svolgere vanno adottate dall'organo o dalle persone fisiche cui è attribuita la gestione dell'ente (es. Consiglio Direttivo o c.d.a., il Presidente, ecc.);
- che gli adempimenti richiesti dal GDPR devono ovviamente essere attuati da persone fisiche (ad es. il Presidente, un consigliere delegato, i dipendenti, o anche i volontari);
- che i limiti imposti dal GDPR vanno rispettati da chiunque nell'ETS utilizzi dati personali;
- che, infine, le responsabilità civili, amministrative e penali in caso di violazione del GDPR gravano non solo sulla persona giuridica ma anche, in varia misura, sugli amministratori/consiglieri/persone fisiche che hanno malamente agito o hanno omesso di adottare le misure di sicurezza necessarie.

Posto che per il GDPR il **Titolare** (cd. "data controller") è la persona giuridica che decide che trattamento di dati svolgere e come svolgerlo ("determina le finalità e i mezzi del trattamento di dati personali"), deve esser considerata Titolare del trattamento anche la **sezione locale** o l'**organismo periferico di una Associazione** qualora eserciti un **potere decisionale sostanzialmente esclusivo e autonomo sui trattamenti dei dati**, con tutte le relative conseguenze (deve pertanto predisporre una propria informativa, deve chiedere il consenso al trattamento, deve tenere se del caso il Registro del Trattamento, ecc.).

In molti casi, tuttavia, è evidente l'esigenza che il trattamento dei dati all'interno di una organizzazione no profit complessa e ramificata sia uniforme e sia deciso di comune accordo tra gli enti che ne fanno parte. Si pensi a tutte le organizzazioni che presentano appunto vari livelli territoriali (es. comunale, provinciale, regionale e nazionale) e che scambiano tra loro i dati dei soci, a maggior ragione se l'adesione del socio ad un ente di primo livello determina anche l'adesione all'ente di livello superiore.

Quando le decisioni sulle finalità e sui mezzi/modalità del trattamento vengono assunte insieme, gli enti coinvolti si definiscono **CONTITOLARI DEL TRATTAMENTO** e ai sensi dell'art. 26 GDPR devono redigere e sottoscrivere un apposito **ACCORDO DI CONTITOLARITA',** nel quale descrivere le finalità e modalità dei trattamenti, i ruoli, i rapporti e le relative responsabilità in relazione agli obblighi derivanti dal GDPR (informative, rapporti con gli interessati, misure di sicurezza informatiche, prassi organizzative comuni o uniformi, ecc.).

6. Quali sono i principi e i limiti con cui gli ETS devono trattare i dati personali?

Ai sensi dell'art. 5 del RGDP le ODV, le APS ed in generale gli ETS, come qualsiasi titolare:

→ devono trattare i dati in modo **lecito** e secondo **correttezza** e **trasparenza**;
→ possono raccogliere i dati solo per **finalità** determinate, esplicite e legittime, ed utilizzare i dati solo in termini compatibili con tali scopi ("**limitazione delle finalità**");
→ devono assicurarsi che i dati raccolti siano adeguati, pertinenti e non eccedenti rispetto a quanto necessario per il perseguimento delle finalità per cui sono raccolti ("**minimizzazione dei dati**");
→ siano esatti e, se necessario, costantemente aggiornati ("**esattezza dei dati**");
→ devono conservarli per un periodo di tempo non superiore a quello necessario per il raggiungimento delle finalità per cui sono stati raccolti, a meno che la conservazione non avvenga per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ("**limitazione della conservazione**");
→ devono garantire un'adeguata sicurezza e protezione dei dati personali, mediante misure tecniche e organizzative adeguate, per evitare trattamenti non autorizzati o illeciti e per evitare la perdita e la distruzione accidentale dei dati ("**integrità e riservatezza**")

Il **PRINCIPIO DI FINALITÀ** resta anche per il Regolamento UE uno dei fondamenti del trattamento dei dati.

Significa che **la raccolta dei dati e il loro successivo utilizzo devono avere precise e determinate finalità, che vanno comunicate all'interessato e poi rispettate**. **Per gli ETS le finalità del trattamento dei dati tendenzialmente coincidono o sono compresi negli scopi istituzionali indicati nello statuto** (anche se lo statuto è spesso generico, e le finalità del trattamento vanno specificate nell'informativa)

Quindi ad esempio quando l'associazione raccoglie i dati comuni dei suoi associati per inserirli nel libro soci, per inviare a casa la corrispondenza o il giornalino dell'associazione e comunque per averne la reperibilità, o raccoglie i dati dei beneficiari dell'attività per garantire il servizio, ***non potrà senza l'autorizzazione specifica ai soci/beneficiari usare tali dati per scopi diversi da quelli istituzionali****: ad esempio non potrà comunicare il nome e l'indirizzo o altre informazioni a terzi per marketing, iniziative commerciali o comunque per scopi che non riguardano l'ente.*

Il **PRINCIPIO DI MINIMIZZAZIONE** (E PROPORZIONALITA') viene anch'esso confermato e valorizzato dal GDPR, e impone agli ETS di non acquisire informazioni e dati ultronei rispetto a quelli necessari per il raggiungimento degli scopi del trattamento.

Nella prassi capita varie volte che le Associazioni sottopongano agli utenti o a coloro che entrano in contatto con l'Ente moduli nei quali conferire un numero o tipologie di dati eccessivi rispetto alle finalità (es. nelle richieste di iscrizione alla newsletter, o nella domanda di partecipazione ad un evento o a un seminario sono da considerarsi certamente ultronei la residenza, la data di nascita e il C.F. insieme, o due recapiti telefonici, ecc.). In tali casi va valutato di volta in volta quali siano i ***dati strettamente indispensabili per fornire il servizio richiesto****; è però certamente possibile, nello stesso modulo (es. modulo o format di iscrizione ad un corso), proporre all'interessato di conferire i dati ulteriori e di fornire il consenso al trattamento per diversi servizi cui voglia accedere (es. facilmente chi partecipa ad un corso organizzato dall'Associazione acconsentirà a che il suo indirizzo mail sia inserito nella newsletter che lo avverta di nuovi eventi formativi).*

Gli altri principi dell'art. 5 verranno affrontati nel proseguo del presente lavoro.

7. Le Associazioni e gli ETS devono fornire all'interessato l'informativa? Con che contenuto e modalità?

L'informativa è una **comunicazione** che serve per far conoscere all'interessato come il Titolare gestisce e utilizza i dati che lo riguardano. È inoltre il **presupposto essenziale** perché l'interessato possa dare il **consenso**/autorizzazione al trattamento, quando questo è richiesto dalla legge.

Permane anche in base al GDPR, l'obbligo di fornire l'informativa all'interessato.
L'informativa va comunicata/consegnata ai **soci e/o volontari**, ai **collaboratori esterni**, ai **dipendenti**, ai **beneficiari e a tutti coloro di cui l'Associazione/ETS acquisisce, conserva e utilizza dati personali**, che si possono definire "interessati".
Le informative redatte e trasmesse in base al Codice italiano (art. 13 D.Lgs. n. 196/2003) **vanno integrate in base al contenuto dell'informativa descritto all'art. 13 del GDPR e ritrasmesse agli interessati** (salvo ovviamente non presentassero già allora il contenuto ora richiesto dal GDPR).

L'informativa deve contenere:
a) l'identità e i dati di contatto del **titolare del trattamento** e, ove applicabile, del suo rappresentante;
b) i dati di contatto del **responsabile della protezione dei dati (Data Protection Officer o DPO)**, ove nominato;
c) le **finalità** del trattamento cui sono destinati i dati personali nonché la **base giuridica** del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) (esistenza di un "*legittimo interesse del titolare del trattamento o di terzi*" che non leda i diritti e le libertà fondamentali dell'interessato), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Inoltre, la stessa informativa deve contenere:
a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del **diritto dell'interessato** di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sul consenso prestato dall'interessato (ai sensi dell'6 comma 1 lett. a e art. 9 comma 2 lett. a del GDPR), l'esistenza del **diritto di revocare il consenso** in qualsiasi momento, senza però pregiudicare la liceità del trattamento effettuato sulla base del consenso prestato prima della revoca;
d) il diritto di proporre reclamo al Garante della Protezione dei Dati Personali;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, commi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il GDPR (art. 12 comma 1) prevede che l'informativa sia concisa, trasparente, comprensibile, facilmente accessibile e di linguaggio semplice e chiaro e sia fornita "**per iscritto o con altri mezzi**" e anche "se del caso, con **mezzi elettronici**" e anche **oralmente**, "se richiesto dall'interessato".

L'informativa (insieme al consenso, ove richiesto) costituisce per le associazioni, soprattutto le più piccole, un'incombenza burocratica. È utile tener presente che:

→ **ogni qualvolta l'Associazione debba richiedere all'associato o all'utente o a qualsiasi interessato anche il consenso al trattamento dei dati**, e vi sia la possibilità di incontrare fisicamente la persona e sottoporle un modulo cartaceo, l**a relativa richiesta di consenso e la firma dell'interessato saranno poste nel**

modulo cartaceo subito dopo l'informativa, e l'interessato firmando il consenso dichiarerà anche di aver letto l'informativa

→ quanto invece il consenso non è necessario, l'interessato potrà ugualmente firmare l'informativa cartacea per "presa visione", oppure l'informativa potrà essere spedita **via e-mail** (in questo caso può essere opportuno chiedere al destinatario di rinviare un messaggio di "conferma", che l'ente potrà stampare o comunque conservare);

→ l'informativa **vale per tutti i trattamenti futuri** che riguardano l'interessato, e va quindi **fornita una sola volta**, se il trattamento dei dati non cambia e rispetta le finalità indicate nell'informativa medesima;

→ l'informativa **deve essere comunicata solo a quei soggetti dei quali l'associazione raccoglie, registra o utilizza i dati**, e tra costoro non rientrano quindi i beneficiari dell'attività istituzionale che l'ente non identifica.

La comunicazione/consegna va fatta nel momento in cui l'interessato fornisce i suoi dati: in pratica la prima volta che la persona viene a contatto con l'ente. Se i dati non sono forniti dall'interessato ma da altre persone/soggetti, l'obbligo dell'informativa all'interessato va adempiuto, ai sensi dell'art. 14 comma 3 GDPR, entro un mese o nel momento in cui i dati vengono comunicati per la prima volta all'interessato o a terzi.

*Sono invece **sconsigliabili** altre forme di informativa quali:*

- *l'affissione nei locali della sede, che potrebbe tutt'al più "coprire" alcuni soci abituali, ma non i beneficiari ed in genere le persone che non accedono alla sede dell'associazione;*
- *l'inserimento dell'informativa nello statuto dell'associazione, le cui modifiche oltretutto sono decise dall'assemblea con maggioranze particolari, con evidenti problemi nel caso il trattamento di dati si svolga poi in termini diversi da quelli inizialmente descritti;*
- *l'inserimento/pubblicazione dell'informativa all'interno del giornale/notiziario dell'associazione (o allegata allo stesso), che consente di informare solo coloro che ricevono il giornalino (avuto riguardo oltretutto che ai sensi dell'art. 13 del GDPR l'informativa va comunicata/consegnata nel momento appena precedente a quello in cui l'interessato fornisce i suoi dati all'associazione).*

*Opzione valida (in relazione però ai soli trattamenti per cui non è necessario acquisire il consenso) è invece la **pubblicazione dell'informativa nel sito istituzionale**, scelta espressamente prevista dal GDPR (58° considerando). Tale comunicazione può assumere varie forme:*
*a) un'**informativa generale** che riguarda tutti i trattamenti svolti dall'Associazione, articolata in più "strati" estensibili in modo tale che l'interessato possa arrivare facilmente ai trattamenti che lo riguardano;*
*b) **specifiche informative** che vengono visualizzate (pop-up) quando l'utente del sito compila un format per richiedere un'attività o un servizio (es. richiesta di iscrizione a socio o richiesta di un servizio), con le quali viene informato sul trattamento dei dati conferiti nel format (meglio se l'invio del format sia preceduto dalla conferma di avvenuta lettura mediante apposito flag);*
*c) l'utilizzo di **icone standardizzate** (di cui è prevista anche la definizione da parte della Commissione Europea) che presentino i contenuti dell'informativa in forma sintetica, in combinazione però con la possibilità di accedere all'informativa estesa.*

*Sempre in tema di informativa presente nel sito web, va tenuta presente la diversità tra l'informativa da rendere all'interessato in ordine ai trattamenti di dati svolti dall'Associazione per lo svolgimento dell'attività sociale/istituzionale o per adempiere ad una richiesta di servizio e l'**informativa specifica sul trattamento dei dati degli utenti del sito web** (utilizzo dei cookies, profilazione dell'utente, ecc.), nella prassi inserita nella home page dei siti (nel "piè di pagina" o "footer") attraverso il link "privacy" o "privacy policy".*

Infine, il GDPR consente anche altre forme di informativa (vocale, via telefono, attraverso messaggi registrati o mediante QR Code, ecc.) che richiedono un approccio tecnico più complesso ma anche, in ogni caso, l'accortezza di poter poi dimostrare che l'informativa è stata resa.

ATTENZIONE: all'informativa va accompagnata la **richiesta di consenso al trattamento dei dati** in tutti i casi in cui questa è da considerarsi obbligatoria o è consigliata.
I MODELLI di sola informativa o di informativa e consenso sono indicati alla fine della D/R n.11.

8. Cosa si intende per "categorie particolari di dati"? Sono i vecchi "dati sensibili"?

Il Codice italiano definiva dati sensibili quei dati "idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o

organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (art. 4, lett. d).

Il GDPR contiene, all'art. 9, una definizione (analoga) di "**categorie particolari di dati personali**", che comprendono:
- **DATI SENSIBILI**, che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale"
- **DATI GENETICI** e **DATI BIOMETRICI** intesi a identificare in modo univoco una persona fisica
- **DATI SANITARI** (e cioè i dati relativi alla salute) o quelli relativi alla vita sessuale o all'orientamento sessuale della persona.

I dati "particolari" riguardano la sfera più intima dell'individuo e pertanto richiedono una particolare protezione, o perché dati che il soggetto ha interesse a non diffondere o perché informazioni che, se apprese al di fuori di un determinato contesto, possono essere causa di atteggiamenti discriminatori.

Le Associazioni e ETS possono facilmente avere a che fare con dati "particolari" (sensibili)*: quelli dei beneficiari dell'attività sociale, quando operano proprio nei settori che il legislatore considera più delicati, come ad esempio l'ambito sanitario e della salute (ad es. chi lavora con malati, soggetti diversamente abili o tossicodipendenti, ma anche con anziani portatori di patologie), l'ambito religioso o caratterizzato ideologicamente in senso politico, ma anche filosofico (ad es. un'associazione espressamente e "istituzionalmente" pacifista o antiproibizionista), l'ambito dell'appartenenza etnica (es. associazioni che lavorano con i nomadi o migranti).*

In base all'art. 9 del GDPR si deve ritenere che sia dato "particolare" la stessa informazione circa l'appartenenza di una persona ad una **associazione/ente che abbia carattere istituzionalmente religioso o filosofico**, mentre **non sembra essere un dato "particolare" l'informazione dell'appartenenza a quelle associazioni (la maggior parte) che si richiamano genericamente a doveri e principi di solidarietà e altruismo**.

9. Sono ancora valide le Autorizzazioni Generali del Garante italiano? Ci sono regole particolari per il trattamento dei dati "particolari" da parte degli ETS?

L'art. 26 del Codice italiano prevedeva che i dati "sensibili" potessero essere trattati solo previa autorizzazione del Garante per la protezione dei dati personali, e a tal fine il Garante aveva emesso (e di volta in volta rinnovato), prima dell'entrata in vigore del GDPR, varie **AUTORIZZAZIONI GENERALI**, tra cui l'**autorizzazione n. 3 del 15.12.2016** al "trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni".

Dopo l'abrogazione dell'art. 26 da parte del D.Lgs. n. 101/2018, il **Garante**, ai sensi dell'art. 21 dello stesso D.Lgs. n. 101/2018, ha individuato, con **provvedimento/autorizzazione generale del 5.6.2019**, le parti della "vecchia" autorizzazione n. 3 che risultano "*compatibili*" con le norme del sopravvenuto GDPR.

In sostanza il Garante ha confermato/precisato che il trattamento da parte degli ETS dei dati "particolari" (ex sensibili) deve considerarsi autorizzato se segue le seguenti regole/principi:

- ✓ sono autorizzati a trattare dati "particolari" tutti gli **ETS** (associazioni anche non riconosciute, organizzazioni di volontariato e promozione sociale, in generale organizzazioni del Terzo Settore, incluse le loro federazioni, fondazioni e ONLUS, cooperative sociali, chiese, associazioni o comunità religiose);
- ✓ il trattamento dei dati sensibili può essere effettuato "per il perseguimento di **scopi determinati e legittimi individuati dalla legge, dall'atto costitutivo, dallo statuto** o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di patrocinio, di tutela dell'ambiente e delle opere d'interesse artistico e storico, di salvaguardia dei diritti civili, di beneficenza, assistenza sociale o socio-sanitaria"

  Tale elencazione, che comprende la maggior parte delle attività/scopi degli ETS, non è per la verità perfettamente allineata con gli artt. 5 e 6 del Codice del Terzo Settore sulle "attività di interesse generale" e sulla "attività diverse" degli ETS; si deve ritenere comunque ammesso il trattamento dei dati sensibili

nell'ambito di tutte attività di interesse generale e connesse degli ETS iscritti ai registri e prossimamente al RUNTS.

- ✓ **quando ETS si avvalgono di terzi** (società, liberi professionisti) per svolgere le loro attività o per la tenuta dei registri e scritture contabili o per la gestione amministrativa o per l'adempimento di obblighi fiscali o la diffusione di riviste, bollettini e simili o per ottenere beni o servizi, possono comunicare a detti terzi (che siano titolari autonomi del trattamento) i relativi dati "particolari" (dei soci/aderenti, dei beneficiari, dei lavoratori, ecc.) strettamente indispensabili allo svolgimento di detti servizi/attività, redigendo previamente un "***atto scritto*** *che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo e le particolari misure di sicurezza adottate*" e inserendo nell'informativa ex art. 13 GDPR resa agli interessati (soci/aderenti, beneficiari, lavoratori, ecc.) l'indicazione di detti terzi e le finalità per le quali essi utilizzano i loro dati

  Risulta oscura tale previsione, in quanto da una parte non si comprende in che modo ad esempio gli obblighi fiscali debbano richiedere un trattamento di dati "particolari" (e non di semplici dati comuni); dall'altra non è comunque chiarito in che termini i soggetti terzi possano considerarsi Titolari autonomi del trattamento e non invece Responsabili (esterni) del trattamento ex art. 28 GDPR (vedi par. n. 15). In ogni caso il Garante consente agli ETS di predisporre semplicemente una ***lettera scritta diretta al proprio consulente/fornitore*** *nella quale indicare i dati che saranno comunicati, le finalità e le modalità con le quali li può utilizzare e le misure di sicurezza necessarie.*

- ✓ gli ETS possono **comunicare i dati "particolari" di un singolo socio/aderente agli altri soci/aderenti** senza il suo consenso solo se tale comunicazione è prevista dallo Statuto ed è effettuata per il perseguimento di scopi determinati e legittimi e se l'informativa ai soci indica le modalità di utilizzo dei dati. Se tuttavia i dati riguardano "profili esclusivamente personali riferiti agli associati/aderenti", l'ETS deve utilizzare "forme di consultazione individualizzata", adottando ogni misura opportuna per evitare che i dati vengano conosciuti da soggetti diversi dal richiedente/destinatario.

  Posto che tendenzialmente gli Statuti degli ETS non regolano l'aspetto relativo alla condivisione dei dati tra soci, il Garante impone di chiedere il consenso del socio (una volta per tutte nella domanda di adesione oppure ogni volta si renda necessaria la condivisione), anche quando la condivisione dei suoi dati (es. cellulare o mal) è strettamente funzionale ad esempio all'organizzazione del servizio associativo istituzionale (es. turni di presenza).

  Quanto alle informazioni inerenti "profili esclusivamente personali" del socio, esse possono riguardare ad esempio eventuali violazioni e procedimenti disciplinari a carico del socio o situazioni inerenti alla sua salute (es. infortunio occorso durante il servizio). È evidente che in tali casi la riservatezza del socio va tutelata anche se egli ha prestato il generale consenso alla condivisione dei suoi dati con gli altri soci (ad. esempio le informazioni sulle violazioni disciplinari andranno comunicate solo ai membri dell'organo chiamato a giudicarlo e i dati sanitari solo a chi all'interno dell'Associazione deve valutare l'idoneità al servizio).

- ✓ Gli ETS possono **comunicare i dati "particolari" di un socio/aderente all'esterno o diffonderli** solo con il consenso degli interessati e solo se tale comunicazione/diffusione è strettamente pertinente/indispensabile rispetto alle finalità perseguite, e nell'informativa devono essere precisate le tipologie di destinatari e le finalità della trasmissione.

Il rispetto delle prescrizioni contenute nelle autorizzazioni generali è di una certa importanza, in quanto ai sensi dell'art. 21 comma 5 D.Lgs. n. 101/2018 la loro violazione comporta l'applicazione della **sanzione amministrativa** di cui all'art. 83 comma 5 GDPR.

10. Le Associazioni ed ETS devono chiedere il consenso all'interessato per il trattamento dei suoi dati personali "comuni" e "particolari"?

Il GDPR prevede varie ipotesi in cui il trattamento dei dati comuni e "particolari" (ex sensibili) può avvenire anche senza il consenso dell'interessato.

In particolare, **il consenso non è necessario** quando il trattamento dei **DATI COMUNI** (art. 6 GDPR):

- è necessario per adempiere ad un **obbligo legale** imposto dal diritto dell'UE o dalla legge dello Stato membro;

- è necessario per l'**esecuzione di un contratto** del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- è necessario per l'esecuzione di **compiti di interesse pubblico**;
- è necessario per il perseguimento del **legittimo interesse del titolare del trattamento o di terzi** che non lega i diritti e le libertà fondamentali dell'interessato (es. le campagne di raccolta fondi).

Parimenti, il consenso non è necessario quando il trattamento dei **DATI PARTICOLARI** (art. 9 GDPR):

- riguarda dati particolari dei "**dei membri, ex membri e delle persone che hanno regolari contatti** con l'ente", se tale utilizzo è svolto nell'ambito dell'attività e finalità dell'associazione e con adeguate garanzie (di protezione dei dati), **con divieto però di comunicazione e diffusione all'esterno**.
- è necessario per gli adempimenti in materia di diritto del lavoro, sicurezza sociale e protezione sociale;
- è necessario per tutelare un interesse vitale dell'interessato o di altra persona fisica, e costoro non possano prestare il consenso;
- riguarda dati "resi manifestamente pubblici dall'interessato".

Come visto (vedi par. n. 11) il Garante ha precisato con il provvedimento/autorizzazione generale del 5.6.2019, le specifiche condizioni nelle quali gli ETS possono trattare i dati "particolari".

Le norme di cui sopra consentono quindi all'ODV, APS ed ETS di **non chiedere il consenso**:

- ✓ per il trattamento dei dati comuni e "particolari" (anche sanitari) dei propri dipendenti/lavoratori se è necessario per l'adempimento degli obblighi nascenti dal **rapporto di lavoro** (nel rispetto del provvedimento/autorizzazione generale del Garante del 5.6.2019, riferito anche al trattamento dei "dati particolari" nei rapporti di lavoro);
- ✓ per la comunicazione dei dati comuni (dei soci/aderenti, dei beneficiari, dei lavoratori) ai propri fornitori/consulenti, se indispensabile al raggiungimento degli scopi istituzionali, nel rispetto del provvedimento/autorizzazione generale del Garante del 5.6.2019, riferito anche al trattamento dei dati particolari da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose
- ✓ per la comunicazione obbligatoria dei dati comuni all'Agenzia delle Entrate;
- ✓ per la comunicazione dei dati comuni degli associati alla compagnia di assicurazione da parte delle ODV ed ETS iscritti ai registri del volontariato (e in futuro al RUNTS) per l'**assicurazione obbligatoria**;
- ✓ per il trattamento dei dati COMUNI serve per eseguire un servizio richiesto dal beneficiario (es. richiesta di trasporto o assistenza domiciliare);
- ✓ per il trattamento di dati particolari/sensibili serve per la tutela della vita o incolumità fisica della persona;
- ✓ per il trattamento di dati comuni avviene per campagne di raccolta fondi (fermo restando il diritto dell'interessato di opporsi).

Nelle suddette ipotesi di esonero dal consenso non rientra però, ad esempio, la **pubblicazione dei dati personali** (tra i quali vi sono anche le **immagini, foto, video,** ecc.) **nel sito istituzionale o nei social network** (es. pagina Facebook) dell'Associazione. Si tratta infatti di una vera e propria diffusione di dati alla generalità delle persone per la quale si deve ritenere necessaria l'acquisizione di **previo e specifico consenso** dell'interessato (da rilasciare ad esempio con specifica sottoscrizione al momento della presentazione della domanda di iscrizione a socio). Si veda sul punto la D/R n. 30.

Come si può vedere, le ipotesi di esonero dal consenso sono comunque particolari e di non immediata identificazione, e quindi **acquisire il consenso** dell'interessato, soprattutto se si trattano suoi DATI PARTICOLARI (ex sensibili) **è sempre consigliato** quando si ha la possibilità di incontrarlo fisicamente e fargli firmare per consenso/autorizzazione.

E va comunque tenuto presente:

- → che anche nel caso non si debba o voglia chiedere il consenso, **va sempre fornita all'interessato l'informativa,** nella quale descrivere specificamente le modalità con cui l'ETS utilizza i dati
- → che **i dati sanitari** e quei dati idonei a rivelare la vita sessuale **non possono essere diffusi nemmeno su consenso dell'interessato**.

11. Come va richiesto il consenso per il trattamento dei dati "comuni" e "particolari"?

Ecco le caratteristiche del consenso descritte all'art. 7 del GDPR:

- **espresso**, cioè esplicito e manifestato in modo inequivocabile (non può essere desunto da un comportamento indiretto o dal silenzio)
- **libero**, cioè manifestato liberamente dal soggetto, richiesto in termini non definitivi e non incondizionati. Inoltre, il consenso non può essere imposto se invece è facoltativo (ad esempio l'Associazione non potrà imporre all'aderente, quale condizione per l'iscrizione a socio, di prestare il consenso al trattamento dei suoi dati per finalità estranee a quelle istituzionali)
- **specifico**, ovvero riferito ad uno o più trattamenti individuati e aventi specifiche finalità, e descritti con linguaggio semplice e chiaro
- **informato**, ovvero preceduto dall'informativa di cui all'art. 13
- **sempre revocabile** (ovviamente la revoca non comporta l'illegittimità dei trattamenti svolti in precedenza).

Quanto alla forma del consenso, il GDPR non impone sia scritto, ma impone al titolare di "**essere in grado di dimostrare" di averlo ottenuto**, e quindi è consigliabile ottenere una sottoscrizione dell'interessato o comunque conservare prova dell'avvenuta autorizzazione.

Si possono a tal proposito utilizzare gli accorgimenti già individuati a proposito dell'informativa, anche perché la richiesta e dichiarazione di consenso deve essere sempre preceduta/accompagnata dall'informativa.

Quindi:

→ *per quanto riguarda i nuovi soci/aderenti**, l'informativa e la dichiarazione di consenso possono essere allegati o contenuti nella domanda di adesione all'associazione**, o scritti nel retro*

→ *la richiesta di consenso può essere anche spedita **via mail**, con la richiesta all'interessato di inviare una mail (non automatica) di "conferma" (che l'ente potrà stampare e conservare), quando però gli sia stato reso chiaramente noto che il messaggio di risposta sarà inteso quale autorizzazione al trattamento*

→ *se l'associazione gestisce un sito web esiste la possibilità di utilizzare il cd. **point&click**, ovvero di creare attraverso appositi software una pagina web nella quale l'interessato può accedere per fornire i propri dati personali, per essere informato delle modalità del trattamento, e soprattutto per autorizzare il trattamento barrando una o più caselle (**che non sia già "preflaggate"**). Tale operazione rende molto semplice per le associazioni la raccolta dei dati, la comunicazione dell'informativa e l'acquisizione del consenso e si traduce in un buon risparmio di tempo per chi richiede e fornisce il consenso; importa però una certa spesa e l'intervento di un tecnico informatico, poiché richiede il rispetto di alcuni precisi requisiti di sicurezza e riservatezza delle transazioni informatiche, da valutare a seconda della tipologia dei dati forniti. È pertanto consigliata solo per le grandi associazioni*

→ *il consenso va acquisito **una sola volta** se il trattamento dei dati non cambia e rispetta le finalità indicate nell'informativa medesima*

→ *il consenso va richiesto **solo a quei soggetti dei quali l'Associazione/ETS raccoglie, registra o utilizza i dati**, e tra costoro non rientrano ovviamente i soggetti beneficiari dell'attività istituzionale che l'ente non identifica*

→ *se l'associazione ha chiesto e ottenuto il consenso nel vigore del Codice italiano non ha l'obbligo di acquisirlo nuovamente, a meno che i trattamenti che svolge si siano a tal punto modificati da richiedere un'autonoma manifestazione di volontà dell'interessato.*

*Come è ovvio, l'acquisizione del consenso è abbastanza semplice se l'interessato è un socio o un collaboratore dell'associazione; se invece è un **beneficiario** (si pensi ad esempio ad una persona anziana) potrebbero sorgere problemi e comunque un adempimento burocratico poco si adatta alla situazione. Certo che, se si ritiene necessario il consenso (perché il trattamento non rientra nelle ipotesi di esclusione o perché si ritiene comunque di acquisirlo), il mezzo più sicuro, anche in relazione ai dati comuni, è la sottoscrizione dell'interessato della relativa dichiarazione, perché consente al Titolare di dimostrare di averlo ricevuto.*

Con riferimento agli interessati che siano **MINORENNI, il consenso va prestato da coloro che esercitano la responsabilità genitoriale** o, se esiste, dal tutore. Il Codice italiano all'art. 2 quinquies consente espressamente che il consenso possa essere rilasciato dai minori che abbiano almeno 14 anni solo con riferimento all'"**offerta diretta di servizi della società dell'informazione**" (che sono quei servizi definiti all'articolo 1, par. 1 lett. b) della direttiva UE 2015/1535 come i servizi forniti "a distanza, per via elettronica e a richiesta individuale": le piattaforme web, i social network, i servizi digitali in genere).

*Spesso ci si chiede se il consenso per il trattamento dei dati del figlio minorenne vada sottoscritto da **entrambi i genitori** o sia sufficiente la firma di **uno solo**. Regola generale è quella per cui, a prescindere dallo stato di convivenza, matrimonio, separazione o divorzio, i genitori devono assumere insieme le scelte di "straordinaria amministrazione" (e cioè quelle di maggiore interesse per il minore, attinenti all'istruzione, educazione, salute e residenza abituale), mentre le decisioni ordinarie e quotidiane possono invece essere assunte anche da uno solo dei due genitori. Non è semplice capire se il consenso al trattamento dei dati personali sia una decisione di ordinaria o straordinaria amministrazione, e non è determinante che il GDPR, all'art. 8 comma 2, parli al singolare di "titolare della responsabilità genitoriale". Si consiglia comunque di prestare particolare attenzione alle richieste di consenso ai trattamenti di dati sensibili o che comportano una diffusione dei dati o immagini del figlio. Nel caso in cui non vi sia la possibilità o l'intenzione di acquisire il consenso di entrambi i genitori, può essere utile inserire nella formula del consenso la precisazione per cui la firma dell'unico genitore viene apposta "in conformità alle norme sulla responsabilità genitoriale di cui agli artt. 316, 337 ter e 337 quater del codice civile" (in sostanza, di comune accordo con il genitore che non firma e/o non si rapporta con l'Associazione).*

La dichiarazione di consenso va fatta sottoscrivere personalmente all'interessato e deve essere preceduta dall'informativa di cui all'art. 13 del GDPR. In tal caso, invece di firmare per "presa visione" dell'informativa, l'interessato firmerà per autorizzazione/consenso al trattamento, dichiarando che il consenso è reso dopo aver letto l'informativa.

Si allegano al presente lavoro i seguenti **ESEMPI E MODELLI DI INFORMATIVA E (OVE NECESSARIO O CONSIGLIATO) della relativa richiesta di CONSENSO AL TRATTAMENTO, da utilizzare, integrare e modificare in relazione alla specifica realtà associativa**:

1. **DOMANDA DI AMMISSIONE A SOCIO CON INFORMATIVA E CONSENSO**
2. **DOMANDA DI AMMISSIONE A SOCIO MINORENNE CON INFORMATIVA E CONSENSO**
3. **INFORMATIVA E CONSENSO per BENEFICIARI**
4. **INFORMATIVA E CONSENSO per BENEFICIARI MINORENNI**
5. **INFORMATIVA PARTECIPAZIONE EVENTO CON FOGLIO PRESENZE E CONSENSO**
6. **INFORMATIVA per CONSULENTI, COLLABORATORI E FORNITORI**
7. **INFORMATIVA per DIPENDENTI, TIROCINANTI E SERVIZIO CIVILE**
8. **INFORMATIVA per UTENTI SITO INTERNET**
9. **INFORMATIVA per ISCRITTI ALLA NEWSLETTER**

12. I dati vanno aggiornati? Possono essere conservati anche dopo la cessazione del rapporto associativo?

L'**aggiornamento o rettifica dei dati** (art. 16 GDPR) deve essere svolto quando è necessario per il corretto raggiungimento delle finalità del trattamento o per soddisfare una legittima esigenza dell'interessato.

Chiaramente è interesse dell'associazione/ETS far sì che le informazioni relative ai soggetti con cui e a favore di cui opera siano aggiornati, e nella pratica ciò avviene comunemente, per iniziativa dell'associazione o dell'interessato che comunica le variazioni intervenute (es. cambio di indirizzo o di indirizzo e-mail). L'aggiornamento/rettifica dei dati è anche un vero e proprio diritto dell'interessato.

Quanto al problema della **conservazione dei dati**, soprattutto alla luce del nuovo GDPR ci si deve chiedere se l'associazione possa trattenere e utilizzare i dati personali dei propri associati anche dopo che essi hanno lasciato l'Associazione.

Come visto (D/R n. 10) il GDPR (art. 9 comma 2 lett. d) consente alle *"fondazioni, associazioni o organismi senza scopo di lucro"* l'**utilizzo dei dati degli ex membri/soci** senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'Ente e con adeguate garanzie (di protezione dei dati), con **divieto però di comunicazione all'esterno** (per tale comunicazione ci vuole il consenso specifico dell'ex socio). Deve quindi ritenersi certamente ammissibile la conservazione di un Albo d'oro, come anche può ritenersi consentito l'uso dei dati del socio per attività specifiche a lui rivolte (es. invio della newsletter, convocazione per gli anniversari, ecc.). In applicazione del principio di proporzionalità e minimizzazione dei dati, i dati "trattenuti" dall'associazione dopo l'uscita del socio dovranno però essere strettamente inerenti alle specifiche attività "residue", e quindi potranno per esempio ridursi al nominativo e all'indirizzo mail.

Quindi:

- **nell'informativa di cui all'art. 13 GDPR va specificato quali dati l'associazione intende conservare anche dopo la cessazione del rapporto associativo**, fermo restando l'avvertimento all'interessato che comunque, in ogni caso, il socio cessato potrà chiederne la cancellazione;
- dei dati del socio cessato è comunque **vietata la comunicazione all'esterno o la diffusione** (salvo esplicito consenso del socio);
- con le opportune cautele per evitarne la diffusione, l'associazione potrà, secondo i principi di cui sopra, conservare una sorta di "**albo d'oro**" con i nominativi di coloro che sono stati soci, attraverso una rubrica o albo cartaceo (o attraverso lo stesso libro soci "storico") conservati in luogo non accessibile a terzi.

La conservazione dei dati degli ex soci è esigenza sentita dalle Associazioni, che desiderano anche solo avere traccia di coloro che hanno "transitato" all'interno dell'ente. Si tratta di un aspetto comunque delicato, soprattutto con riferimento a quei dati considerati "sensibili", in quanto idonei "a rivelare l'adesione ad associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale". Si capisce che la diffusione o la comunicazione a terzi di una precedente iscrizione ad una associazione, soprattutto se di ispirazione religiosa, filosofica, politica o sindacale, di una persona che ad un certo punto ha deciso di non farne più parte potrebbe essere considerata illecita e comunque non gradita all'interessato.

*Quanto ai soggetti che eseguono abitualmente o periodicamente **donazioni** di denaro all'associazione o all'ETS, potrebbero considerarsi, ai sensi dell'art. 9 comma 2 lett. d) GDPR, persone che hanno "contatti regolari" con l'ente. In questo caso la conservazione dei dati e l'utilizzo (es. banca dati dei donatori) può avvenire senza il consenso, se i dati personali non vengono comunicati all'esterno.*

*Quanto invece ai dati dei **beneficiari dell'attività**, salvo non vi siano specifici obblighi di legge di conservazione, essi vanno cancellati quando l'attività o il servizio nei loro confronti debba intendersi definitivamente esaurito, salvo un espresso loro consenso di un trattamento ulteriore (es. invio di campagne di raccolta fondi, aggiornamento sulle ulteriori iniziative dell'Associazione, ecc.).*

13. Quali sono i diritti degli interessati nei confronti dei Titolari che trattano i dati? Esistono nuovi diritti?

La protezione dei dati è assicurata all'interessato anche attraverso l'esercizio dei diritti indicati dagli articoli da 15 a 22 del GDPR.

In base a tali articoli **l'interessato può infatti chiedere al Titolare** (e quindi all'ente non profit):

- di avere conferma che l'ente utilizza i suoi dati e di sapere quali siano questi dati;
- di conoscere l'origine dei dati (cioè come e da chi l'ETS li ha acquisiti), le finalità del trattamento, i soggetti a cui i dati vengono comunicati e il periodo di conservazione dei dati;
- di rettificare (correggere o integrare) i dati inesatti o incompleti (es. cambio di indirizzo o dello stato civile, aggiornamento del curriculum, ecc.);
- di cancellare i dati (cd. **diritto "all'oblio**") quando il trattamento non è più necessario per il raggiungimento delle finalità per cui sono stati raccolti, o in caso di revoca del consenso, o in caso di trattamento illecito o negli altri casi previsti dall'art. 17 GDPR;
- di ottenere una "limitazione del trattamento" nei casi previsti dall'art. 18 GDPR;
- di poter trasferire i dati ad un altro titolare (diritto "alla **portabilità** dei dati");
- di opporsi al trattamento dei suoi dati, anche se svolto correttamente dall'associazione, se sussistono "motivi particolari" (cioè particolari e valide ragioni: ad esempio se ha presentato domanda di recesso dall'associazione, o se il trattamento, anche se lecito, risulta lesivo della sua dignità o riservatezza);
- di opporsi al trattamento dei dati svolto per il "**marketing diretto**" (invio di materiale pubblicitario o vendita diretta o compimento di ricerche di mercato o di comunicazione commerciale);
- di non essere sottoposto ad una decisione basata su un "trattamento automatizzato" di dati (inclusa la cd. profilazione).

Quindi **ogni persona può chiedere ad ogni Titolare** (es. banca, datore di lavoro, azienda, ente pubblico o privato, ODV/APS, ETS, ecc.) **se e in che modo il Titolare utilizza suoi dati personali e di esercitare i suddetti diritti, e anche gli ETS, quali Titolari, potrebbero ricevere tale richiesta**. Le modalità di esercizio di tali diritti devono essere esplicitate nell'informativa (generalmente si indica un indirizzo di posta elettronica o

un contatto telefonico o un numero di fax o la lettera raccomandata): **si consiglia all'associazione di individuare una persona/Incaricato cui attribuire il compito di evaderla**.

Si ricordi che per l'Associazione/ETS sono **"interessati" anche gli associati/volontari**, e non solo i soggetti esterni all'ente.

14. Le Associazioni e gli ETS devono nominare un "Responsabile della Protezione dei Dati" (Data Protection Officer - DPO)?

L'art. 37 del GDPR introduce la figura nuova, non prevista dal Codice italiano del 2003, del "Responsabile della Protezione dei Dati".

Per evitare di confonderlo con il "Responsabile del trattamento dei dati", si consiglia di utilizzare la dicitura inglese di "**Data Protection Officer**" abbreviato in "**DPO**".

Si tratta di una persona interna o esterna al Titolare o anche di una società esterna a cui spettano compiti di controllo e assistenza sui trattamenti svolti dal Titolare, al fine di assicurare che tali trattamenti siano conformi al GDPR.

L'art. 37 stabilisce che siano obbligati a nominare il DPO:

a) gli enti pubblici;
b) i (Titolari) privati che hanno come attività principale lo svolgimento di "trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala";
c) i (Titolari) privati la cui attività principale consiste "nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

Anche dopo due anni dall'entrata in vigore del GDPR, non sono stati esplicitati criteri specifici e oggettivi per determinare quando un trattamento di dati è svolto "**SU LARGA SCALA**". Certamente vanno utilizzati criteri quantitativi e qualitativi, attinenti al numero degli interessati, al numero di dati trattati, all'estensione temporale e geografica del trattamento. Le Linee Guida europee (Article 29 Data Protection Working Party) hanno indicato a titolo esemplificativo come soggetti che svolgono trattamenti su vasta scala gli ospedali, le aziende di trasporto, le compagnie assicurative e gli istituti di credito, i fornitori di servizi di telecomunicazione.

Posto che un ETS non ha natura pubblica ai sensi dell'art. 37, lett. a) GDPR e difficilmente svolge come attività principale un "monitoraggio delle persone su larga scala" ai sensi dell'art. 37, lett. b GDPR (es. scoring o profilazione o attività predittive sulla persona; osservazione, monitoraggio o controllo sistematico degli interessati anche attraverso reti e app; controllo a distanza dell'attività di dipendenti; uso di tecnologie innovative come sistemi di intelligenza artificiale, scanning vocale e testuale; interconnessione, combinazione o raffronto di informazioni), **devono valutare se nominare un DPO quegli ETS che trattano SU LARGA SCALA dati "particolari" (ex sensibili) e dati giudiziari**, a maggior ragione se relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

È quindi probabile che siano tenute a nominare un DPO le organizzazioni no profit di grandi dimensioni o strutturate in più livelli o in più regioni o province, che trattano i dati di un numero considerevole di aderenti (soprattutto se tali ETS presentano chiara ispirazione politica, filosofica, religiosa o sindacale) o di beneficiari, o i cui livelli o strutture territoriali mettano in comune i dati "particolari" dei propri soci o dei beneficiari, oppure quegli ETS la cui attività in ambito sanitario (es. donazione del sangue, assistenza sanitaria e trasporto sanitario) comporti un trattamento sistematico o comunque importante di dati.

15. Cosa si intende per "Responsabile del Trattamento"?

Ai sensi del vecchio Codice italiano, ogni Titolare poteva nominare, anche all'interno della propria organizzazione o Ente, uno o più Responsabili del Trattamento, e cioè una o più persone deputate a svolgere compiti di responsabilità, organizzazione e direzione sui trattamenti dei dati. Sono stati così nominati Responsabili del trattamento i dirigenti dei vari settori dell'impresa o le figure apicali degli uffici amministrativi degli enti pubblici o anche qualche membro del Consiglio Direttivo di ODV o APS.

L'art. 28 del GDPR prevede effettivamente la figura del "**Responsabile del Trattamento**" inteso come una **persona fisica o giuridica** (es. società) **che svolge, su incarico scritto del Titolare o sulla base di un contratto, un trattamento dei dati "per conto" del Titolare**.

Gli interpreti sono concordi nel ritenere che il "Responsabile del Trattamento" in base all'art. 28 GDPR è solo quel **soggetto esterno al Titolare che svolge un trattamento di dati per conto e su incarico del Titolare, quale suo delegato**. Quindi non devono essere nominati Responsabili né il Presidente, né i Volontari, né i responsabili di Sezioni della stessa Associazione, né i dipendenti in posizioni apicali o di responsabilità, né probabilmente i lavoratori autonomi (es. psicologi, medici, operatori, ecc.), trattandosi di persone interne all'Ente o comunque incardinate nella struttura gerarchica o organizzativa dell'Ente, le quali vanno invece semplicemente istruite come Autorizzati al trattamento.

La nomina a Responsabile (esterno) deve risultare da un contratto/atto scritto nel quale il Titolare definisce le caratteristiche e i limiti del trattamento dei dati che dovrà essere svolto dal Responsabile e nel quale il Responsabile si impegna ad adottare adeguate misure di sicurezza ai sensi dell'art. 32 GDPR per evitare la perdita, la distruzione o l'accesso indesiderato ai dati, nonché a collaborare con il Titolare nel rispetto degli obblighi di legge. Tale contratto/atto potrà essere un appendice/allegato o inserito come parte del contratto "sostanziale" nel quale vengono stabilite le condizioni della fornitura/servizio/attività.

Anche in relazione all'attività degli ETS, non è però così semplice capire quando questo soggetto esterno delegato (ditta individuale, società, professionista, ecc.) debba essere nominato Responsabile ex art. 28 GDPR (con la necessità di stipula di apposito contratto/atto) o possa restare anch'esso un Titolare soggetto autonomo che semplicemente tratta i dati comunicati dall'ETS.

Tendenzialmente si può dire che il soggetto terzo assume il ruolo di Responsabile quando svolge una attività che è propria (istituzionale o tipica o necessaria) dell'Associazione/ETS, ma di cui quest'ultima si "spoglia" in tutto o in parte delegandola a detto esterno.

Trattasi però di situazioni da valutare di volta in volta, ed infatti:

→ il Garante ha escluso che le **Compagnie assicurative** debbano essere nominate Responsabili del trattamento dai soggetti assicurati (in relazione ai dati degli assicurati/beneficiari della polizza), posto che l'attività assicurativa è attività propria di dette Compagnie e non è attività delegata dell'assicurato (parere Garante 21.10.2019);

→ lo stesso Garante ha invece precisato che il **Consulente del Lavoro** vada nominato Responsabile del trattamento in relazione alle attività svolte per conto del cliente concernenti la gestione degli adempimenti contabili e amministrativi per i lavoratori del cliente (es. redazione buste paga), posto che trattasi di attività delegata (esternalizzata) dal cliente datore di lavoro nell'ambito di proprie scelte organizzative (parere Garante 22.1.2019).

→ ma soprattutto lo stesso Garante, nel **provvedimento/autorizzazione generale del 5.6.2019** (vedi par. n. 11) ha precisato che **quando ETS si avvalgono di terzi** (società, liberi professionisti) per svolgere le loro attività o per la tenuta dei registri e scritture contabili o per la gestione amministrativa o per l'adempimento di obblighi fiscali o la diffusione di riviste, bollettini e simili o per ottenere beni o servizi, **ove tali soggetti debbano considerarsi Titolari autonomi del trattamento**, il trattamento dei dati "particolari" necessari allo svolgimento di tali attività debba essere regolato da un "***atto scritto*** *che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo e le particolari misure di sicurezza adottate*" e tali soggetti indicati nell'informativa ex art. 13 GDPR resa agli interessati.

Infine, ove l'Associazione avesse prima del GDPR nominato uno o più Responsabili interni del trattamento ai sensi dell'art. 29 del Codice italiano, questa designazione non sembra incompatibile con il GDPR: si consiglia però, ad evitare confusioni, che il vecchio Responsabile del Trattamento sia chiamato **Delegato al Trattamento** (o Responsabile **interno** del trattamento) o ancor meglio si individuasse per lui un apposito profilo di **Autorizzato**.

Da ultimo, **le Associazioni/ETS possono essere loro stesse nominate Responsabili del trattamento** qualora svolgano un'attività delegata da altri soggetti Titolari che comporti il trattamento di dati personali. Sono identificabili due principali situazioni:

a) trattamenti svolti dall'Associazione locale per conto della "casa madre", quando non sia configurabile un rapporto di Contitolarità;

b) trattamenti svolti dall'Associazione/ETS nell'ambito di una attività svolta per un ente/committente privato o per un Ente Pubblico nell'ambito di una convenzione o di un appalto. Si veda la D/R n. 28.

Si allega al presente lavoro un esempio/modello di
10. ACCORDO/INCARICO AL RESPONSABILE ESTERNO DEL TRATTAMENTO
11. ISTRUZIONI A TERZO TITOLARE AUTONOMO
da utilizzare, integrare e modificare in relazione alla specifica realtà associativa

16. Esiste ancora la figura dell'Incaricato del Trattamento?

La figura dell'Incaricato del Trattamento non è espressamente prevista dal GDPR, che all'art. 29 fa solo riferimento a "soggetti istruiti" dal titolare del trattamento.

Il Codice italiano, nella versione aggiornata al GDPR, all'art. 2 terdecies e art. 14 comma 1 lett. i) parla di **persona AUTORIZZATA o designata al trattamento dei dati personali sotto l'autorità diretta del Titolare**.

Nonostante l'assenza di specifiche indicazioni nel GDPR e nel Codice, è evidente che il Titolare deve provvedere ad individuare le persone incaricate/designate, a indicare loro le finalità, i limiti e le modalità dei trattamenti che andranno a svolgere e a istruirle, anche perché **la previsione e il rispetto di procedure sugli incaricati/designati** garantisce una migliore dimostrazione, da parte del Titolare, di aver adottato le MISURE ADEGUATE di trattamento dei dati.

Sono possibili due soluzioni:
- **nominare come Incaricato o Autorizzato** al trattamento ciascun soggetto che all'interno e per conto dell'Associazione tratta dati personali (Presidente, consiglieri, Volontari, dipendenti, ecc.)
- in alternativa alla nomina individuale, predisporre una policy (istruzioni operative, regolamento interno, ecc.) sul trattamento dei dati svolto dalle varie **categorie** di soggetti che operano all'interno dell'Associazione.

È in ogni caso utile rispettare i seguenti accorgimenti:
- gli incaricati/autorizzati operano sotto la diretta autorità del Titolare, attenendosi alle istruzioni impartite
- la nomina/ designazione è effettuata **per iscritto** e individua puntualmente i trattamenti consentiti, le banche dati/sistemi informatici a cui può accedere
- la nomina degli incaricati/autorizzati, con le opportune istruzioni, è **necessaria anche se la persona esegue solo trattamenti "cartacei"** e non informatici. Quando la persona utilizza il computer, la sua designazione e la delimitazione del suo trattamento rientra nel cd. sistema di autorizzazione (**vedi par. 19**)
- il titolare potrà consegnare all'incaricato/autorizzato una **LETTERA DI INCARICO/NOMINA D AUTORIZZATO** nella quale lo designa come tale, indica che trattamenti egli può svolgere, di quali dati, con quali modalità e nel rispetto di quali misure di sicurezza. Se l'incaricato/autorizzato svolge un trattamento informatico i "confini" del saranno corrispondenti al "profilo di autorizzazione" (vedi D/R n. 19). Chiaramente se i profili sono uguali le lettere di incarico potranno avere lo stesso identico contenuto anche se intestate e consegnate a diversi soggetti.

Infine, come detto alla D/R n. 15, ove l'Associazione avesse prima del GDPR nominato uno o più Responsabili interni del trattamento ai sensi dell'art. 29 del Codice italiano, potrà rinominarli Autorizzati con un particolare profilo di autorizzazione/responsabilità.

Sembra invece si possa prescindere da una vera e propria "lista degli incaricati" prevista dal punto 15 del "vecchio" Disciplinate Tecnico, soprattutto ove venga adottato il Registro dei Trattamenti. Ove si volesse provvedere, si ricorda che tale lista, che si potrà chiamare anche **ORGANIGRAMMA PRIVACY**, deve essere aggiornata periodicamente (almeno una volta all'anno): può essere o **nominativa** o individuare **classi omogenee** (es. volontari/aderenti, dipendenti, membri del Consiglio, ecc.), e deve anche contenere i nominativi degli addetti alla gestione e manutenzione degli strumenti elettronici (compreso quello precedentemente detto "amministratore di sistema").

Si allega al presente lavoro un esempio/modello di
12. **ATTO DI NOMINA A INCARICATO/AUTORIZZATO AL TRATTAMENTO**
13. **ORGANIGRAMMA PRIVACY**
da utilizzare, integrare e modificare in relazione alla specifica realtà associativa.

Infine, sempre ai fini della dimostrazione di aver adottato tutte le MISURE ADEGUATE, va assicurata la **formazione degli Incaricati/autorizzati** sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili del GDPR più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano. La formazione va programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. È utile che la formazione svolta venga documentata, per poter dimostrare che è stata posta in essere.

Si allega al presente lavoro un esempio/modello di
14. **PIANO DELLA FORMAZIONE**

17. Cosa sono i dati giudiziari? Possono essere trattati dagli ETS?

Il Codice italiano definiva **dati giudiziari** quei "dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale".

La norma del Codice è stata abrogata in sede di recepimento, e quindi il trattamento dei dati giudiziari si deve ora fondare solo sulla previsione dell'art. 10 del GDPR, secondo cui:

"**il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza** sulla base dell'articolo 6, paragrafo 1, **deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri** che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".

Il Codice italiano riformato dal D.Lgs. n. 101/2018 prevede inoltre, all'art. 2 octies, che nel caso il trattamento dei dati giudiziari non sia previsto da alcuna norma di legge (o, su previsione di legge, da un regolamento), esso può avvenire solo se autorizzato con decreto del Ministero della Giustizia, sentito il Garante.

*Sono quindi **dati giudiziari** tutte le annotazioni (di natura penale) che risultano dal **casellario giudiziale**, tra cui le sentenze di condanna e i decreti penali irrevocabili, le misure di sicurezza poste a carico di un individuo, i provvedimenti di amnistia e ogni altro dato relativo "ai reati". Non invece le sentenze e i provvedimenti civili.*

In definitiva, il trattamento di dati giudiziari è ora possibile se si rientra nelle ipotesi di liceità dell'art. 6 GDPR e se è presente almeno una di queste condizioni:

a) se il trattamento avviene "**sotto il controllo dell'Autorità pubblica**"
b) **o se il trattamento è autorizzato dal diritto dell'Unione o dal diritto italiano** che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

*Entrano a contatto con dati giudiziari le associazioni (o anche le cooperative sociali) che operano nella **realtà carceraria** o che accolgono persone che hanno subito una condanna penale (ammessi a **lavori di pubblica utilità** quali sanzioni sostitutive di pene brevi o misure alternative alla detenzione) o persone che scelgono la "**messa alla prova**" come misure per evitare la condanna. Le suddette ipotesi erano espressamente previste nell'**autorizzazione generale n. 7/2016** del Garante italiano (che consentiva appunto il trattamento di dati giudiziari dei soci e dei beneficiari a quegli Enti del terzo settore "che curano il patrocinio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi, quanto il trattamento è indispensabile per perseguire scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo"), ma tale autorizzazione è divenuta inefficace con l'entrata in vigore del D.Lgs. n. 101/2018.*

In ogni caso, deve ritenersi che le ipotesi di trattamento dei dati giudiziari per le finalità sopra descritte (messa alla prova, lavori di pubblica utilità, ecc.) siano del tutto legittime, sia perché il coinvolgimento degli enti del terzo settore è espressamente **previsto dalla legge**, sia perché l'attività (e il relativo trattamento dei dati) avvengono sotto il **controllo del Ministero della Giustizia** (U.E.P.E.) e del **Tribunale** territoriale con il quale gli enti no profit sono tenuti a stipulare apposite convenzioni.

In ogni caso, e soprattutto al di fuori delle ipotesi sopra indicate, si consiglia a tutti gli ETS che svolgono la loro opera a favore di persone trattando loro dati giudiziari di **collegare ogni attività di trattamento ad un chiaro**

e preventivo controllo dell'ente pubblico che mette a disposizione questi dati e di esplicitare nei rapporti con l'Ente pubblico, con gli interessati e i terzi le **finalità di interesse pubblico** delle attività che richiedono il trattamento di tali dati.

18. Cosa sono le misure di sicurezza "adeguate"? Sono sufficienti le vecchie misure "minime" di sicurezza per la protezione dei dati personali?

Il Codice italiano definiva **MISURE DI SICUREZZA** gli accorgimenti, procedure e strumenti di custodia e controllo informatico e non informatico dei dati che hanno lo scopo di "ridurre al minimo i rischi di distruzione e perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta".

Questa definizione può essere tendenzialmente conservata, ma **va invece assolutamente abbandonata la differenza tra MISURE MINIME DI SICUREZZA** (quelle indicate dal Codice e dal vecchio cd. "Disciplinare Tecnico" come necessarie ad assicurare un livello minimo di protezione la cui mancata adozione era colpita da sanzione penale: es. assegnazione di password agli incaricati/autorizzati, installazione di antivirus) **e le MISURE DI SICUREZZA IDONEE** (tutte quelle che, ulteriori rispetto alle minime perché corrispondenti allo stato della tecnica, erano comunque da adottarsi per ridurre al minimo i rischi del trattamento, e la cui mancata adozione comportava anche il rischio di dover risarcire in sede civile i danni subiti da terzi).

Il GDPR (art. 24 e 33) non prevede che le misure di sicurezza siano definite dalla legge o da un documento tecnico, ma **assegna al Titolare la totale responsabilità di individuare tutte le MISURE TECNICHE E ORGANIZZATIVE ADEGUATE alla propria attività**, tenendo conto dello stato dell'arte e dei costi di attuazione; della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento; dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

e ciò al fine:

→ "di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente" al GDPR
→ "di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"
→ di assicurare "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico";
→ di assicurare "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

Tale **RESPONSABILIZZAZIONE** o **RENDICONTAZIONE** ("**ACCOUNTABILITY**", termine usuale per il non profit) implica quindi:

1. l'adozione e il costante aggiornamento di prassi, procedimenti, strumenti tecnici e informatici specifici e prestabiliti, e cioè previsti, progettati e posti in essere **prima** dell'attività di trattamento (cd. **PRIVACY BY DESIGN**)
2. che tali accorgimenti siano introdotti quale "impostazione predefinita" del sistema, tale che un trattamento non conforme sia rifiutato dal sistema (cd. **PRIVACY BY DEFAULT**)
3. la redazione e conservazione di idonea **DOCUMENTAZIONE** (es. linee guida o regolamenti interni, contratti scritti di incarico con la ditta di software, istruzioni operative, ordini di servizio, ecc.) che valga a dimostrare verso l'esterno di aver approntato tali misure.

Ma come potrà un ETS essere certo di aver adottato le MISURE ADEGUATE?

a) innanzitutto, non c'è dubbio che qualsivoglia trattamento informatico di dati non possa ormai prescindere dall'adozione delle vecchie "misure minime", e cioè dalla predisposizione:
   - di un sistema di **AUTENTICAZIONE INFORMATICA** (vedi D/R n. 18) di **AUTORIZZAZIONE** e di **PROTEZIONE** del sistema informatico da virus e accessi indesiderati, al fine di "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"
   - un sistema di conservazione dei dati attraverso **COPIE DI SICUREZZA**, per poter "ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico";

b) il GDPR precisa poi che un elemento per dimostrare l'avvenuta adozione delle misure adeguate consiste nell'adesione ai cd. **CODICI DI CONDOTTA** (di futura emanazione) o a un **MECCANISMO DI CERTIFICAZIONE** (di futura predisposizione)

c) ulteriori strumenti e metodi sono indicati all'art. 26 e 32 del GDPR nell'ambito del principio cd. della "PRIVACY BY DEFAULT", e sono:

- la **PSEUDONIMIZZAZIONE** (conservazione separata dei dati dell'interessato tale che un solo dato non ne consente l'identificazione), la **MINIMIZZAZIONE** (eliminazione dati inutili, generalizzazione dei dati rimasti) e la **CIFRATURA** dei dati personali (trasformazione del dato in una sequenza apparentemente casuale di numeri e lettere e segni che sono riconvertitili nel dato originario solo con apposita chiave);
- le misure tecniche e organizzative dirette a garantire che, "per impostazione predefinita", siano svolti solo i trattamenti di dati (per quantità di dati, periodo di conservazione e accessibilità) corrispondenti alle specifiche finalità del trattamento;
- le misure tecniche e organizzative dirette a garantire che, "per impostazione predefinita", non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica;
- l'adozione di una **PROCEDURA PER TESTARE**, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Infine, alle Associazioni ed ETS che trattano DATI SANITARI va segnalato che l'art. 2 septies del Codice italiano (riformato) assegna al Garante il compito di stabilire periodicamente (per adeguarle allo stato della tecnica) la MISURE DI GARANZIA/SICUREZZA per il trattamento di tali dati, con riferimento ad esempio ai "profili organizzativi e gestionali in ambito sanitario" e alle comunicazioni della diagnosi.

19. Che cos'è un sistema di autenticazione informatica?

Consiste essenzialmente nell'attribuzione al soggetto o ai soggetti che all'interno dell'associazione gestiscono i dati mediante computer (Incaricati/autorizzati) delle cd. *credenziali di autenticazione*, ovvero di un codice o di un dispositivo di identificazione personale, in modo che solo questi soggetti e non altri estranei possano accedere ai computer e gestire i dati secondo i loro compiti e l'ambito a loro attribuito.

I codici di identificazione più semplici sono quelli basati sul sistema **USERNAME** e **PASSWORD**; i più sicuri sono invece quelli che sfruttano le caratteristiche biomediche (voce o impronta del pollice). Chiaramente la prima soluzione è quella meno dispendiosa. **L'username non può essere assegnato a diversi incaricati/autorizzati, nemmeno in tempi differenti**.

Quanto alle **password**, generalmente sono determinate pensando alla data di nascita, ai familiari, a parole di senso comune. Tuttavia, queste password non sono sicure, perché facilmente decifrabili.
Valgono tuttora per le password le indicazioni del vecchio Disciplinare Tecnico, opportunamente integrate, e quindi è assai consigliato:

- che la password sia di almeno 8 caratteri (oppure del numero di caratteri massimo consentito dallo strumento elettronico) e non contenga elementi facilmente ricollegabili alla persona del suo utilizzatore/incaricato
- che sia composta da numeri e lettere insieme (maiuscole, minuscole) e da simboli
- che sia conosciuta solamente dall'incaricato e quindi memorizzata dall'incaricato/utilizzatore del computer o conservata in modo da impedire la conoscenza di estranei *(es. busta chiusa in un cassetto chiuso, oppure conservata da una sola persona con opportune cautele)*
- che sia personale e assegnata a più incaricati/autorizzati *(non sono quindi ammesse password di gruppo)*
- che sia sostituita/modificata dall'incaricato al primo utilizzo [*nei sistemi informatici complessi*] e successivamente almeno ogni tre mesi
- che sia disattivato l'accesso dell'utente quando il possessore delle credenziali cessa dalla qualità di incaricato (es. ex dipendente o ex socio) o quando l'accesso non è più effettuato per un certo periodo (es. maternità o malattia di una dipendente, infortunio).

L'individuazione iniziale delle password e degli *username* è generalmente svolta da un soggetto esterno esperto informatico, che nel passato è stato identificato nell'**Amministratore di Sistema** previsto *dal DPR 318/99, non più previsto nell'attuale Codice italiano (e nemmeno nel GDPR). Ciò non toglie che, nei fatti, ci possa essere e anzi sia* ***consigliabile il suo intervento****: si tratta infatti del tecnico o della ditta che adatta il sistema*

*informatico alle esigenze del Titolare, suggerendo le **MISURE ADEGUATE** in relazione ai trattamenti (informatici) svolti dall'Associazione.*

Se all'interno dell'Associazione esistono le competenze tecniche per predisporre le misure adeguate, l'intervento di un esterno non sarà necessario e amministratore di sistema sarà colui (dipendente, volontario) che se ne occupa. Ma attenzione, il suo intervento dovrà essere comunque professionale, e l'Associazione Titolare non potrà gestire tale intervento in forme "amicali", ma dovrà conservare traccia documentale degli interventi svolti (es. dichiarazione del tecnico), al fine poi di poter dimostrare l'adozione delle misure adeguate.

Le modifiche successive della password spettano invece in teoria al solo Incaricato; per favorire tale operazione i computer possono generalmente essere impostati in modo tale che richiedano periodicamente al proprio utilizzatore di cambiare la password.

20. Che cos'è un sistema di autorizzazione informatica?

Si ha quando il sistema informatico predisposto dal Titolare **distingue due o più "profili", ovvero due o più ambiti diversi in cui si svolgono i trattamenti elettronici di dati** all'interno dell'associazione, qualora il Titolare decida che uno o alcuni Incaricati/autorizzati possano svolgere solo determinati trattamenti e quindi possano accedere solo ad alcuni ambiti o programmi o banche dati, secondo il proprio "profilo". I profili possono riguardare ciascun incaricato/autorizzato ma anche "classi omogenee" di incaricati/autorizzati, e devono essere individuati prima del trattamento.

Un esempio può chiarire meglio: una associazione può decidere che il semplice aderente/volontario non possa accedere ai computer o possa lavorare solo su alcuni dati, senza avere accesso informatico a tutti i dati dell'associazione, ai rendiconti, ai verbali ecc., o che gli eventuali dipendenti accedano a banche dati diverse o tra loro o rispetto al Presidente o ai membri del Consiglio. Si tratta di operazioni che richiedono sotto il profilo tecnico l'installazione di un server o comunque l'impostazione di diversi profili/utenti e quindi l'intervento di un tecnico informatico. L'accesso ai dati conservati nel sistema informatico locale deve essere quindi regolato da opportune credenziali e non lasciato accessibile mediante il semplice accesso alla rete medesima.

La predisposizione di un sistema di autorizzazione è necessaria solo se ci sono più "profili": **il titolare infatti può anche decidere che tutti gli incaricati/autorizzati accedano a tutti gli ambiti del trattamento che si svolge nella sua struttura** (cioè a tutte le banche dati o a tutti i programmi): in questo caso non sarà necessario un "sistema" perché il profilo di autorizzazione sarà unico (uno stesso profilo per tutti gli incaricati/autorizzati).

In presenza di un unico profilo, l'eventuale "sbarramento" potrà essere posto a monte: **il titolare potrà cioè decidere di far accedere ai computer solo una ristretta cerchia di persone**, le sole cui saranno assegnate le credenziali di autenticazione (*Username* e *password*) necessarie ad usare i computer. Queste persone avranno tutte lo stesso "profilo", e potranno accedere all'intero sistema.

Ci si chiede: in caso di unico profilo o di più profili, può l'associazione decidere che, per comodità, la password sia una sola (o una sola per ogni profilo) e, se pur attribuita formalmente ad una sola persona/incaricato, venga conosciuta e utilizzata per l'accesso al/ai computer da tutte le persone dell'associazione che abitualmente li usano?

La risposta a rigore è negativa: a prescindere dall'attribuzione dello stesso profilo a "classi omogenee" di incaricati/autorizzati (es. volontari, membri del Consiglio, dipendenti addetti all'amministrazione), è bene che **a ciascun incaricato siano attribuite autonome e diverse credenziali di autenticazione, cioè un diverso USERNAME e una PASSWORD, per il solo fatto di svolgere un trattamento mediante computer**.

21. Che cos'è un sistema di protezione informatica e di backup?

Un sistema di protezione informatica serve ad evitare o limitare l'attacco di virus o le intrusioni indesiderate ed in genere l'attacco di "programmi pericolosi".

Programmi pericolosi sono quelli (virus, worm, malware, ecc.), che danneggiano file, programmi e sistemi, o si installano nel computer per compiere operazioni all'insaputa dell'utilizzatore (ad esempio attivano automaticamente la connessione ad internet o estraggono dati dal PC all'insaputa del proprietario). I virus "attaccano" automaticamente anche solo sulla base dell'accesso a internet o alla posta elettronica o della "visita" ad un determinato sito.

Se il computer o la "rete" di computer dall'associazione vengono collegati alla rete o hanno un programma di posta elettronica e contengono altresì dati personali (e magari anche sensibili) le misure da adottare dovranno essere più incisive.

Valgono a tal proposito gli accorgimenti previsti dal Codice del 2003 e dal Disciplinare Tecnico:
- un valido e aggiornato **ANTIVIRUS**
- un **FIREWALL** (in inglese "porta antifuoco"), che consente di bloccare le intrusioni dall'esterno da parte di hacker o di software dannosi che utilizzano accessi particolari per recare danno ai computer o controllare ed estrarre le informazioni (spesso il FIREWALL è integrato nel ROUTER messo a disposizione dal provider di internet)
- l'**AGGIORNAMENTO** periodico dei programmi e sistemi operativi, volti a prevenirne la vulnerabilità e a correggerne i difetti, o la **SOSTITUZIONE** dei programmi operativi desueti
- il salvataggio dei dati mediante **COPIE DI SICUREZZA** o **BACKUP**, e cioè nella loro memorizzazione in banche dati portabili, chiavette USB, dischetti o supporti rimovibili, da conservarsi in un luogo diverso da quello dove si trovano i computer che contengono i dati originali (per evitare, ad esempio, che un incendio possa distruggere entrambi). Si consiglia almeno di formare delle copie di backup contenenti le banche dati (es. dei soci) e i documenti principali (es. verbali di assemblea).
- **DISTRUGGERE I SUPPORTI ESTERNI** quando non sono più utilizzati o cancellarne definitivamente il contenuto quando sono utilizzati da altri soggetti.

L'adozione delle misure sopra descritte richiede, se non si è esperti di computer, l'assistenza di un tecnico informatico. A maggior ragione per le misure di protezione informatica sono importanti i requisiti di professionalità del tecnico (o Amministratore di Sistema), ed è necessario che il Titolare, per poter dimostrare di aver adottato le MISURE ADEGUATE, si faccia rilasciare dal tecnico una descrizione scritta dell'intervento effettuato nella quale il tecnico dichiari di aver dotato il sistema informatico di determinate protezioni e caratteristiche.

Potrà l'Associazione pretendere dal tecnico o dalla società di consulenza o dal fornitore informatico la dichiarazione che le protezioni e le caratteristiche del sistema informatico installato costituiscono MISURE ADEGUATE rispetto ai trattamenti svolti dall'Associazione medesima? Ovviamente sì, ma tale dichiarazione avrà comunque un costo in quanto comporta l'assunzione di responsabilità. Certamente sarà interesse del "tecnico" l'adozione di misure di sicurezza più sicure (e costose), al fine di evitare future responsabilità; l'associazione avrà invece l'esigenza di adottare le misure appena sufficienti per ritenersi "in regola". In ogni caso l'attestazione non libera il titolare dall'onere di mantenere le misure adeguate (ad esempio aggiornare l'antivirus), e il tecnico, naturalmente, non sarà responsabile per modifiche svolte dall'utilizzatore che hanno eliminato le protezioni installate, o se il titolare, dopo l'intervento, decide di svolgere dei trattamenti di dati che richiedono misure più sicure. In generale è consigliato rivolgersi ad un ***tecnico di fiducia****, con cui iniziare un rapporto di collaborazione, e che curi non solo l'installazione ma anche la manutenzione dei sistemi operativi ed elettronici.*

La difesa da programmi pericolosi e virus si attua anche attraverso altri **accorgimenti e attenzioni** da parte dell'incaricato/utilizzatore del computer, non obbligatorie ma consigliabili, come ad esempio:
- non aprire e-mail o allegati dall'incerta o pericolosa provenienza
- non installare programmi scaricati da siti non ufficiali o comunque di natura incerta
- tenere sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti/programmi; disattivare sul browser l'esecuzione automatica degli script Java e Activex
- eseguire periodicamente la pulizia del disco fisso da "cookies", file temporanei ecc.
- evitare i falsi allarmi e le catene di sant'Antonio, controllando preventivamente la bontà delle informazioni prima di diffonderle.

Infine, ma è ovvio, è compito del Titolare istruire gli incaricati/autorizzati affinché **non lascino incustodito e accessibile il computer** durante una sessione di trattamento.

Accorgimenti particolari vanno adottati nel caso in cui l'Associazione, tramite i Volontari o i consiglieri, utilizzi per la gestione dei dati relativi all'attività istituzionale **piattaforme o servizi online, accessibili** non solo dalla sede ma **da qualunque PC o dispositivo (es. smartphone) collegato a Internet**.

In questo caso è importante:
- evitare il più possibile che l'accesso venga svolto mediante **computer di terzi** o comunque sistemi informatici di cui non si possa verificare il sistema di sicurezza e protezione

- **non utilizzare le stesse credenziali** (username e password) **per l'accesso ai diversi servizi online** (es. Posta elettronica dell'Associazione, Facebook, Home banking, Posta elettronica personale, ecc.), in quanto la violazione di uno di questi ambiti potrebbe comportare l'acquisizione da parte di terzi (e il relativo utilizzo) delle password utilizzabili anche per l'accesso agli altri.

22. Cos'è il Registro delle attività di trattamento? È assimilabile al vecchio Documento Programmatico sulla Sicurezza (D.P.S.)?

All'art. 30 il GDPR prevede che alcuni Titolari debbano tenere (e mettere a disposizione del Garante ove richiesto) un Registro delle attività di trattamento, una sorta di "**censimento dei trattamenti**", contenente varie informazioni sui trattamenti svolti, tra cui:
- i riferimenti del Titolare e del DPO se nominato
- le finalità del trattamento
- le categorie di interessati e dei dati personali trattati
- le categorie di destinatari a cui i dati vengono comunicati nonché l'eventuale paese straniero o organizzazione internazionale a cui i dati vengono trasferiti
- il momento della cancellazione dei dati
- se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

La funzione del Registro è riconducibile alla vecchia notifica al Garante dei trattamenti di dati sensibili ai sensi dell'abrogato art. 38 del Codice italiano del 2003, mentre il contenuto è tendenzialmente assimilabile a quello del vecchio DPS (Documento Programmatico sulla Sicurezza), obbligatorio in base al Codice italiano del 2003 e al Disciplinare Tecnico fino all'anno 2012 e poi eliminato.

Ora, nel vigore del GDPR, il Registro rientra tra quegli elementi "documentali" tramite i quali il Titolare dimostra l'adeguamento al DGPR e al tempo stesso lo **strumento operativo principale per avere un quadro dei trattamenti, dei rischi e quindi delle MISURE ADEGUATE da adottare**.

Analogo Registro va predisposto dal Responsabile esterno del Trattamento con riferimento ai trattamenti svolti per conto del Titolare.

Le Associazioni e gli ETS sono tenuti alla redazione e conservazione dei Registri? Non è semplice stabilirlo. L'art. 30 del GDPR stabilisce che non vi sono tenuti gli enti "*con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*".

Quindi **sono tenuti alla redazione del Registro**:
- **sicuramente tutti i Titolari con 250 o più dipendenti** (*situazione difficile a verificarsi con riferimento agli enti no profit, e inoltre considerato il riferimento specifico ai "dipendenti" e quindi alle PMI, si può tendenzialmente escludere che ai dipendenti siano equiparabili i volontari, e quindi che siano tenuti alla redazione del Registro una ODV, APS o ETS per il solo fatto di aver 250 volontari o più*)
- quanto ai **Titolari con meno 250 dipendenti,** l'art. 30 del GDPR identifica delle ipotesi di esenzione, ma non è ancora del tutto chiara la loro portata.
  In particolare, l'opinione maggioritaria ritiene che siano tenuti:
  a) **i Titolari con meno di 250 dipendenti ma i cui trattamenti sono rischiosi per i diritti e le libertà degli interessati** (ipotesi a sua volta assai estesa, perché il 75° Considerando del GDPR stabilisce che vi è rischio ad esempio quando il trattamento può comportare discriminazioni o riguarda dati sanitari o "caratteristici" o se porta alla valutazione della persona o se riguarda minori o se riguarda un numero elevato di interessati); *come anche* **i Titolari con meno di 250 dipendenti ma trattamenti siano continuativi/non occasionali** (anche se non rischiosi); *come anche* **i Titolari con meno di 250 dipendenti ma che trattano dati caratteristici** (ex sensibili) **o giudiziari**.

  Questa interpretazione, avvalorata da Working Party Article 29 (EDPB) comporta in sostanza l'obbligo del **Registro la maggior parte dei soggetti che trattano dati personali** per la loro attività

  b) i Titolari con meno di 250 dipendenti ma i cui trattamenti sono **rischiosi per i diritti e le libertà degli interessati** e sono **continuativi**/non occasionali; *come anche* i Titolari con meno di 250 dipendenti ma i cui trattamenti sono **rischiosi per i diritti e le libertà degli interessati** e, anche se occasionali, riguardano **dati caratteristici** (ex sensibili) **o giudiziari**

Nell'incertezza della norma, e in ogni caso in ragione del fatto per cui facilmente i trattamenti e le attività degli ETS coinvolgono diritti fondamentali o dati sensibili, **si consiglia ad ogni Associazione/ETS di predisporre il Registro**, non solo perché l'omissione a questo obbligo (ove esistente) determina l'applicazione di una sanzione pecuniaria fino a € 10.000.000,00 (!), ma anche perché, ove non inteso in senso burocratico, può costituire un **ottimo strumento** per:

a) rendere chiaro l'assetto privacy dell'ente ai responsabili/consiglieri e a chiunque svolge un trattamento al suo interno
b) stabilire prassi e regole comuni in relazione agli obblighi del GDPR
c) programmare gli eventuali interventi da svolgere sulle misure di sicurezza ove non reputate adeguate

Ecco le principali caratteristiche del Registro:

- deve avere forma scritta, e quindi può essere un **documento cartaceo** o un **documento/file elettronico** da stampare e conservare
- non deve essere comunicato a terzi ma **conservato presso la sede**
- deve essere periodicamente **aggiornato**
  Nulla dice il GDPR sulla frequenza dell'aggiornamento. Tuttavia, si consiglia un aggiornamento "in tempo reale" non appena muti una circostanza ivi descritta, sia perché il Registro va consegnato al Garante in caso di ispezione (e questo comporta la necessità che corrisponda per lo meno negli elementi essenziali allo stato dei trattamenti svolti in quel momento), sia nell'ottica di considerare il Registro uno strumento utile per la gestione del sistema privacy all'interno dell'Associazione
- non è indispensabile abbia "**data certa**", e quindi non vi è necessità di registrazione o invio via p.e.c. a terzi.

Ove l'ETS sia certo che i trattamenti svolti non comportino particolari rischi per gli interessati e non riguardino dati "particolari" (ex sensibili), potrà limitarsi a nominare al proprio interno gli AUTORIZZATI.

In alternativa al Registro dei trattamenti, l'Associazione/ETS potrà redigere e adottare delle **LINEE GUIDA / PRIVACY POLICY**, meglio se approvate con apposita delibera di c.d.a. o Consiglio Direttivo all'inizio di ogni mandato, nelle quali descrivere i principali trattamenti dei dati svolti e le regole e prassi da adottare a cura degli Autorizzati. Questo documento, più discorsivo rispetto ad un vero e proprio Registro, può essere utilizzato per definire l'assetto privacy dell'Ente e come documento formativo/informativo per tutti coloro che all'interno dell'Ente trattano dati personali.

Si allega al presente lavoro un esempio/modello di
15. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO
16. LINEE GUIDA PRIVACY POLICY
da utilizzare, integrare e modificare in relazione alla specifica realtà associativa

23. Quali sono le misure di sicurezza adeguate in caso di trattamento senza mezzi elettronici?

In applicazione dei principi della *privacy by design* e *privacy by default* sopra visti, vanno altresì identificate le principali misure adeguate in caso di trattamento dei dati svolto senza strumenti elettronici.

Si può certamente attingere alle previsioni del Codice del 2003 e del Disciplinare Tecnico, secondo cui:

- vanno fornite **istruzioni scritte agli incaricati/autorizzati** per il controllo e la custodia degli atti e documenti contenenti dati personali
  *Significa che l'associazione deve stabilire le modalità di **custodia, controllo e utilizzo dei documenti** contenenti dati personali (es. se c'è un archivio, chi lo custodisce, chi può accedervi e come, ecc.), dirette ad evitare l'accesso non consentito di terzi estranei. Tali modalità si possono anche solo risolvere nel non lasciare incustoditi presso la sede atti o documenti riguardanti l'ente o gli aderenti e nel riporli in appositi armadi chiusi a chiave, soprattutto se si tratta di dati sensibili.*
- vanno individuati gli **ambiti di trattamento** dei dati consentiti agli incaricati/autorizzati al trattamento o a categorie omogenee di incaricati e il loro aggiornamento almeno annuale
  Significa che l'associazione deve stabilire per iscritto le persone o le categorie omogenee (es. volontari, es. membri del consiglio, es. dipendenti) autorizzate a compiere le attività di trattamento dei dati, con specificazione dei limiti e modalità, e verificare ed eventualmente modificare tali incarichi almeno una volta l'anno. La verifica va fatta per i casi in cui l'incaricato cessi di trattare dati (es. recesso o esclusione

dell'aderente, cessazione delle cariche o degli eventuali rapporti di lavoro ecc.) o venga modificato l'ambito del suo trattamento.

- va assicurato un **accesso controllato** agli archivi e documenti contenenti dati sensibili e/o giudiziari
  Significa che l'associazione deve far attenzione che i documenti/atti contenenti dati sensibili siano accessibili solo alle persone a ciò autorizzate e che costoro non lascino accedere terze persone nel corso del trattamento. L'accesso all'archivio (stanza dove stanno le banche dati cartacee) fuori dall'orario di apertura della sede deve essere registrato in un quaderno.

24. Cos'è la Valutazione di impatto sulla protezione dei dati o DPIA?

Si tratta di una procedura che l'art. 35 del DGPR prevede come sostitutiva del vecchio obbligo del Titolare di notificare al Garante l'esistenza di particolari trattamenti di dati.

Devono fare una Valutazione di Impatto, **prima** di svolgere l'attività di trattamento dei dati, quei Titolari che svolgono trattamenti, specialmente mediante l'uso di **nuove tecnologie**, che, considerati "la natura, l'oggetto, il contesto e le finalità ... possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

In particolare, sono tenuti alla Valutazione di Impatto quei Titolari:

a) che svolgono una **PROFILAZIONE DI DATI**, e cioè raccolgono e raffrontano dati in via automatizzata per compiere una valutazione sistematica e globale di aspetti personali delle persone fisiche, valutazione che poi comporta l'assunzione di decisioni che riguardano significativamente tali persone;
b) che svolgono un trattamento **SU LARGA SCALA** di dati personali "particolari" (sensibili, sanitari, attinenti alla vita sessuale) e giudiziari;
c) che svolgono un'attività di **SORVEGLIANZA** sistematica su larga scala di una zona accessibile al pubblico.

Si tratta di ipotesi che raramente interessano gli Enti del Terzo Settore, ad eccezione del trattamento di dati sensibili e giudiziari, per il quale è necessario capire quanto tale trattamento si svolge su larga scala.

I trattamenti su LARGA SCALA sono stati identificati:

→ nelle Linee Guida dell'organismo europeo *Article 29 Data Protection Working Party*, secondo criteri quantitativi e qualitativi (numero degli interessati, numero di dati, estensione temporale e geografica del trattamento); le Linee Guida indicano a titolo esemplificativo i trattamenti svolti da soggetti quali gli ospedali, le aziende di trasporto, le compagnie assicurative e gli istituti di credito, i fornitori di servizi di telecomunicazione

→ dal Garante per la protezione dei dati personali che, ai sensi dell'art. 35 comma 4 GDPR con provvedimento dell'11.10.2018 ha redatto proprio l'"**Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati**", identificando varie ipotesi tra cui – più vicina al mondo associativo – quella dei **trattamenti non occasionali di dati relativi a SOGGETTI VULNERABILI** (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)" o dei **trattamenti SU LARGA scala di dati "particolari"** (ex sensibili) o di dati giudiziari interconnessi con altri dati personali raccolti per finalità diverse.

Quanto alla procedura vera e propria, si tratta di una sorta di "lente di ingrandimento" sui trattamenti dei dati sopra indicati (e per la verità già descritti se si è redatto un Registro dei trattamenti), poiché è necessario:

a) descrivere i trattamenti e le loro finalità
b) valutare se il trattamento è proporzionato rispetto alle finalità
c) valutare i rischi che il trattamento può comportare per i diritti e le liberta degli interessati
d) valutare se sono necessarie apposite MISURE per affrontare i rischi.

25. Cos'è il Data Breach o "violazione di dati personali"?

Per "Data Breach" o "violazione dei dati personali" (art. 4 e 33 GDPR) si intende una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzato o l'accesso ai dati personali".

Si tratta quindi della perdita, del danneggiamento o della fuoriuscita di dati o dell'accesso illecito anche indipendente dalla volontà dell'Associazione (anche la perdita di una chiavetta USB, il furto del PC, la cancellazione di un archivio dati, l'accesso al computer di estranei, ecc.).

È un **evento che va affrontato subito e che non va nascosto**, in quanto:

- l'occultamento comporta gravi sanzioni (fino a € 10.000.000,00);
- la violazione dei dati, se non bloccata o rimediata, può causare danno all'interessato.

In caso di Data Breach il DGPR prescrive al Titolare (art. 33 e 34):

a) di **denunciare/notificare al Garante** per la Protezione dei Dati Personali l'esistenza della violazione "senza giustificato ritardo e se possibile entro 72 ore" dal momento in cui il Titolare ha conoscenza della violazione medesima.
   L'obbligo di denuncia non sussiste quando sia improbabile che la violazione comporti un rischio/pregiudizio per i diritti e le libertà delle persone (ad esempio se si tratta di dati comuni, o se la violazione consiste nella mera distruzione di dati che possono essere richiesti all'interessato)

b) di **comunicare la violazione all'interessato** "senza ingiustificato ritardo", l'esistenza della violazione che riguarda i suoi dati.
   L'obbligo di comunicazione non sussiste, anche in questo caso, quando la violazione non comporta un rischio/pregiudizio per i diritti e le libertà dell'interessato, e anche negli altri casi di cui all'art. 34 GDPR (ad esempio quanto il Titolare è riuscito ad evitare la lesione dei diritti o la comunicazione richiede sforzi sproporzionati per l'esistenza di un gran numero di interessati).

Consiglieri, volontari e dipendenti vanno tutti responsabilizzati sui rischi di data breach e devono tutti in grado di gestirli, nel senso di essere consapevoli su quello che debba essere fatto in caso di violazione e sugli obblighi di informazione. Le relative istruzioni vanno inserite nella NOMINA AD AUTORIZZATO e se del caso anche nelle LINEE GUIDA PRIVACY POLICY se adottate. Può essere molto utile lasciare traccia delle violazioni intervenute e degli accorgimenti adottati per limitarne gli effetti e per evitare che si ripetano, mediante un **17. REGISTRO DEI DATA BREACH**

26. Quali sono le sanzioni che possono colpire il Titolare in caso di violazione delle norme del GDPR?

Il mancato rispetto delle norme del GDPR può comportare l'applicazione di rilevanti sanzioni penali e amministrative e può causare l'obbligo dell'associazione di risarcire i danni causati a terzi da un trattamento illegittimo.

SUL PIANO PENALE, di competenza di ciascuno Stato membro ai sensi dell'art. 24 GDPR, restano applicabili i REATI previsti dal Codice italiano (D.Lgs. n. 196/2003) che è stato comunque aggiornato al GDPR dal D.Lgs. n. 101/2018.

Trattamento illecito di dati (art. 167)

Reclusione dai 6 ai 18 mesi per chi, al fine di conseguire un profitto proprio o altrui o arrecare danno all'interessato, svolge un trattamento in violazione degli art. 123, 126 e 130 del Codice, ovvero del provvedimento del Garante di cui all'art. 129 del Codice, se ne è derivato un danno all'interessato.
Reclusione da 1 a 3 anni per chi, al fine di conseguire un proprio profitto o altrui o arrecare danno all'interessato, svolge un trattamento di dati sensibili o giudiziari in violazione degli art. 2 sexies e 2 octies del Codice oppure non rispettando le misure di garanzia indicate dal Garante ai sensi dell'art. 2 septies e dall'art. 2 quinquesdecies del Codice, se ne è derivato un danno all'interessato.
Reclusione da 1 a 3 anni per chi, al fine di conseguire un proprio profitto o altrui o arrecare danno all'interessato, trasferisce dati personali fuori dall'Unione Europea o ad un organismo internazionale al di fuori dei casi consentiti dagli artt. 45, 46 o 49 GDPR, se ne è derivato un danno all'interessato

*La prima ipotesi di reato riguarda principalmente i "fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione pubblica accessibile al pubblico" (art. 123 e 126 Codice), la seconda riguarda tendenzialmente le Pubbliche Amministrazioni (art. 2 sexies Codice). Gli ambiti che potrebbero ipoteticamente riguardare un ente no profit sono la violazione dolosa delle regole stabilite dall'art. 130 del Codice sulle "**comunicazioni indesiderate**" automatiche, telefoniche, cartacee o elettroniche, per finalità di marketing, il trattamento di **dati sensibili o giudiziari** non conforme alla legge o in violazione delle misure di sicurezza stabilite dal Garante e il **trasferimento dei dati a paesi extra UE** che non abbiano adottato misure di sicurezza adegate. Tutti i reati presuppongono il*

dolo specifico *di voler arricchire se stessi o altri o procurare un danno e l'esistenza di un pregiudizio (anche non economico) arrecato a terzi.*

Comunicazione o diffusione o acquisizione illecita di dati personali oggetto di trattamento su larga scala (art. 167 bis e 167 ter)

Reclusione da 1 a 6 anni per chi, al fine di conseguire un profitto proprio o altrui o arrecare danno a terzi, comunica o diffonde, in violazione del Codice (art. 2 ter, 2 secties e 2 octies) un "archivio automatizzato" contenete dati trattati su larga scala Reclusione da 1 a 6 anni per chi, al fine di conseguire un profitto proprio o altrui o arrecare danno a terzi, comunica o diffonde, senza il consenso dell'interessato (ove necessario) un "archivio automatizzato" contenete dati trattati su larga scala Reclusione da 1 a 4 anni per chi, al fine di conseguire un profitto proprio o altrui o arrecare danno a terzi, acquisisce con mezzi fraudolenti un "archivio automatizzato" contenete dati trattati su larga scala

Si tratta di ipotesi non perfettamente identificabili, considerata l'incertezza dei concetti di "archivio automatizzato" e di trattamento su larga scala. In ogni caso è richiesto il dolo specifico, e quindi i reati non riguardano condotte contraddistinte dalla mera colpa dei soggetti nel non aver adottato i comportamenti necessari per la diffusione degli "archivi"

Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)

Reclusione da 6 mesi a 3 anni per chiunque, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi in un procedimento davanti al Garante o nel corso di accertamenti eseguiti dal Garante.

Le norme penali parlano genericamente di "chiunque", intendendosi sostanzialmente il Titolare (reato cd. proprio), ma in ogni caso i soggetti che rispondono del reato non sono di facile individuazione. In particolare, quando il Titolare è una associazione, che è una persona giuridica, sorge il problema di individuare la persona fisica responsabile penalmente, poiché la responsabilità penale può colpire solo persone fisiche, salvo casi particolari (di cui al D.Lgs. 231/01) che non riguardano la privacy.

A tal proposito si può dire che, all'interno dell'associazione, la responsabilità penale colpisce chi, sotto il profilo sostanziale, esercita il potere direttivo e ha preso le decisioni in materia di privacy o ha omesso di adottare i comportamenti richiesti dalla legge. Quindi i membri del Consiglio Direttivo, il Presidente dell'associazione, il Responsabile (interno) del trattamento sono le figure più "esposte"; il ***Presidente*** *si potrà liberare da responsabilità dimostrando di aver conferito al Responsabile interno (ad esempio un membro del Consiglio Direttivo) deleghe effettive in materia di privacy, cioè poteri decisionali e di spesa, e dovrà probabilmente dimostrare anche di aver vigilato sull'operato del soggetto delegato. Nel caso del Responsabile interno questa prova liberatoria sarà più difficile: egli dovrà dimostrare che non gli erano state attribuite quelle funzioni il cui scorretto esercizio ha determinato il compimento di un reato. La ripartizione delle responsabilità all'interno dell'associazione è un aspetto molto delicato: si consiglia di attribuirle in relazione all'effettiva competenza e capacità delle persone.*

Ci si può chiedere a questo punto quale sia il ***rischio concreto*** *per le Associazioni e gli ETS in genere di subire un'indagine ed eventualmente una condanna penale. La risposta non è semplice: il Pubblico Ministero, quando ha notizia di un fatto che potrebbe configurare reato, decide se indagare sulla base della gravità del fatto e dell'allarme sociale che tale fatto suscita: in questo senso è più facile che l'accertamento colpisca aziende di grandi dimensioni, o testate giornalistiche, che non una piccola associazione che utilizza un solo computer… Però teoricamente il pericolo esiste, anche in ragione del fatto che le associazioni trattano frequentemente dati sensibili, che sono quelli che vanno maggiormente tutelati.*

Per le associazioni e gli ETS il rischio di una indagine penale potrebbe derivare principalmente dai ***controlli della Guardia di Finanza/Agenzia delle Entrate*** *nell'accertamento del rispetto della disciplina fiscale degli enti non profit: la Guardia di Finanza agisce infatti quale pubblico ufficiale e, se riscontra la possibile esistenza di reati, ha un obbligo di denuncia alla Procura della Repubblica per gli opportuni accertamenti (art. 331 c.p.c.). Tale denuncia spetta anche al Garante ai sensi dell'art. 159, sesto comma del Codice.*

Le **SANZIONI AMMINISTRATIVE** sono previste dall'art. 83 del GDPR e sono le seguenti:

- art. 83 comma 4 GDPR: è soggetta alla **sanzione pecuniaria (multa) "fino a € 10.000.000,00**" la violazione dolosa o colposa degli obblighi gravanti sul Titolare e sul Responsabile del trattamento previsti dagli articoli 8, 11, da 25 a 39, 42 e 43; la violazione degli obblighi stabiliti dall'organismo di certificazione a norma degli articoli 42 e 43; la violazione degli obblighi stabiliti dall'organismo di controllo a norma dell'articolo 41, paragrafo 4.

Si tratta ad esempio delle seguenti ipotesi: trattamento senza consenso dei dati del minore, mancata redazione dei Registri del trattamento o mancata adozione delle MISURE ADEGUATE, mancata notifica al Garante o all'interessato del DATA BREACH, mancata esecuzione della DSPIA, mancata designazione del DPO.
Ulteriori ipotesi, per la maggior parte estranee ai trattamenti svolti dagli enti no profit, sono previste dall'art. 166 comma 1 del Codice aggiornato al GDPR

- art. 83 comma 5 GDPR: è soggetta alla **sanzione pecuniaria (multa) "fino a € 20.000.000,00**" ad esempio la violazione dolosa o colposa:
  a) dei "principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9";
  b) dei "diritti degli interessati a norma degli articoli da 12 a 22";
  c) delle regole per i "trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49";

  Si tratta di tutte le regole e i principi visti nei paragrafi di cui sopra sulla liceità, base giuridica e finalità dei trattamenti, sulla pertinenza ed esattezza dei dati, sul consenso al trattamento dei dati comuni e "particolari", sull'obbligo e contenuto dell'informativa e sugli altri diritti degli interessati (rettifica, oblio, limitazione, portabilità, opposizione).
  Ulteriori ipotesi sono previste dall'art. 166 comma 2 del Codice aggiornato al GDPR.

- art. 83 comma 6 GDPR: è soggetta alla **sanzione pecuniaria (multa) "fino a € 20.000.000,00**" ad esempio la violazione l'inosservanza di un ordine del Garante per la Protezione dei Dati Personali.

Come è facile capire, **si tratta di un apparato sanzionatorio pesantissimo, in quanto commisurato ai giganti della rete** (ad evitare che la sanzione possa essere già prevista a bilancio come rischio necessario e calcolato), **che certamente spaventa le piccole (e grandi) associazioni**.

È possibile che, nonostante le violazioni sopra descritte, il Garante limiti l'importo della sanzione in ragione della natura *non profit* del Titolare o delle ridotte proporzioni dell'Associazione? Tale possibilità non è certa né probabile, tuttavia **il GDPR prevede specifici elementi che possono consentire l'applicazione di una sanzione di basso importo**.

Innanzitutto, si noti che **l'art. 83 non prevede un importo minimo della sanzione**, con ciò ammettendo che possa essere anche di € 100,00 o meno.

Inoltre, la sanzione va determinata tenendo conto i vari elementi, tra cui:
- la non gravità e la limitata durata della violazione
- l'oggetto o la finalità del trattamento (è teoricamente possibile quindi che finalità sociali o benefiche possano temperare la sanzione)
- il limitato numero di interessati lesi o la non rilevanza del danno
- il carattere doloso o colposo della violazione
- le misure adottate dal Titolare per limitare il danno
- il fatto che il Titolare avesse posto in essere misure tecniche e organizzative adeguate
- l'inesistenza di precedenti violazioni
- il fatto che il Titolare abbia cooperato con il Garante al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi
- il fatto che il Titolare abbia spontaneamente notificato la violazione.

Inoltre, va considerato che l'art. 58 GDPR assegna al Garante una serie di **preventivi poteri di controllo** (**avvertimento, ammonimento, ingiunzione/ordine** ad adeguare il trattamento al GDPR, ordine di blocco del trattamento, ecc.) diretti a eliminare quelle condotte del Titolare che potrebbero generare una violazione del GDPR e quindi l'applicazione delle sanzioni.

Le sanzioni amministrative vengono **decise dal Garante per la protezione dei dati personali**, anche su reclamo o segnalazione dell'interessato, dopo una fase istruttoria di accertamento (artt. 166 del Codice aggiornato al GDPR), nella quale il Garante può chiedere al titolare, al responsabile, all'interessato o a terzi di fornire informazioni o esibire documenti. L'irrogazione della sanzione è disciplinata dalla L. n. 689/81 (sulle sanzioni amministrative, es. multe per eccesso di velocità): il Garante, se ritiene si sia compiuto l'illecito, notifica la contestazione; entro 60 giorni chi la riceve può far pervenire sue difese e chiedere di essere sentito; se il Garante conferma la violazione emette una ordinanza ingiunzione di pagamento, che è impugnabile davanti al giudice del luogo in cui è stato commesso l'illecito entro 30 giorni dalla notifica dell'ordinanza.

La responsabilità amministrativa colpisce la persona fisica o le persone fisiche che hanno commesso la violazione (responsabili o incaricati/autorizzati al trattamento); la sanzione però può colpire, ai sensi dell'art. 6 L. 689/81 e a titolo di responsabilità solidale, anche:

a) l'associazione se l'illecito è compiuto dai suoi dipendenti;
b) il proprietario della cosa che è servita a commettere l'infrazione (es. l'associazione quale proprietaria del computer)
c) la persona che aveva la vigilanza su chi ha commesso l'illecito, salvo non provi di non aver potuto impedire il fatto.

In tutti questi casi, però, il responsabile solidale potrà chiedere all'autore dell'illecito l'intera somma che ha dovuto pagare (cd. azione di "regresso").

Non è finita, poiché l'associazione può anche essere colpita da **RESPONSABILITÀ CIVILE** (patrimoniale, da fatto illecito).

L'art. 82 GDPR (che "sostituisce l'art. 15 del Codice italiano, abrogato) prevede infatti che

chiunque subisca un danno materiale o immateriale causato dalla violazione del GDPR (ma anche dalla violazione adottate dagli Stati membri in attuazione del GDPR) ha il diritto di ottenere il risarcimento del danno **dal Titolare** del trattamento o dal **responsabile** del trattamento.

Si tratta di un'ipotesi di responsabilità oggettiva o semi-oggettiva, in quanto:

- deriva dalla mera violazione di una prescrizione del GDPR (anche se è ovviamente necessario che si sia prodotto un danno risarcibile in capo all'interessato e che il danno dipenda dalla condotta del Titolare o del responsabile). In altre parole, non causa responsabilità civile l'aver causato un danno mediante un trattamento di dati (ipotesi prevista dall'abrogato art. 15 del Codice italiano), ma l'aver causato un danno mediante la violazione di una norma del GDPR;
- implica l'inversione dell'onere della prova: **sono il Titolare o il responsabile che, per liberarsi da responsabilità, devono dimostrare "che l'evento dannoso non gli è in alcun modo imputabile**" (art. 82 comma 3 GDPR), e cioè, in sostanza, **di aver adottato tutte le misure idonee ad evitare il danno**: in sostanza, che l'evento dannoso deriva da un evento completamente esterno, o da caso fortuito o forza maggiore, in quanto hanno approntato tutte le MISURE DI SICUREZZA ADEGUATE (tecniche, procedimentali e organizzative) dirette alla tutela dei diritti dell'interessato.

Quindi se una Associazione/ETS viola le norme del GDPR (attraverso i propri amministratori/consiglieri o i responsabili interni o esterni, o le persone autorizzate al trattamento) causando un danno a terze persone, potranno esser chiamate in causa dal danneggiato davanti al giudice civile con una domanda di **risarcimento del danno patrimoniale e/o morale**.

*Questione molto incerta e complessa è quella relativa a quali soggetti siano concretamente tenuti al risarcimento. La tesi più restrittiva è quella per cui, parlando il GDPR esclusivamente e specificamente di "Titolare" (e non di "chiunque"), il danneggiato possa agire solamente nei confronti dell'**associazione** (e quindi rivalendosi, in caso di condanna, solo sul fondo comune), e non nei confronti delle persone fisiche, e ciò anche quando il Titolare sia associazione non riconosciuta. Una seconda tesi, incentrata sulla previsione dell'art. 38 del codice civile (secondo cui delle "obbligazioni" di una associazione non riconosciuta rispondono anche, quali sostanziali fideiussori, "coloro che hanno agito in nome e per conto dell'associazione") o sul principio generale del naeminem laedere di cui all'art. 2043 c.c., prevede che rispondano (oltre all'associazione ai sensi dell'art. 82 GDPR e all'art. 2049 c.c.) anche **il Presidente o soggetti che hanno la rappresentanza dell'associazione, o anche i componenti del Consiglio Direttivo** che avevano il dovere di vigilare o assumere le decisioni dirette al rispetto della norma del GDPR che invece è stata violata, e non hanno invece assunto, con dolo o colpa, le condotte necessarie. Tendenzialmente da escludere, invece, è la possibilità del terzo danneggiato di agire direttamente nei confronti delle persone autorizzate/incaricate del trattamento (che avranno casomai una responsabilità interna verso l'associazione di appartenenza quali lavoratori o associati).*

I principali consigli, quindi, che si possono fornire alle Associazioni ed ETS è quello di:

a) **non sottovalutare l'adeguamento al GDPR**, soprattutto se svolgono trattamenti di **dati particolarmente delicati** (dati "particolari" ex sensibili, dati giudiziari, dati di minori e di persone vulnerabili, dati sanitari, ecc.) o trattamenti di dati di un numero rilevante di persone, specie se con modalità informatiche o "automatiche"

b) **evitare i gravi errori** e la loro ripetizione, che maggiormente possono generare danni ingenti

c) considerare la gestione dei dati personali un **processo di miglioramento continuo** diretto ad evitare i rischi (e soprattutto non nascondere la questione, perché se sorgono violazioni o problemi sarà molto più difendibile la situazione di un Ente che ha perlomeno iniziato un processo di adeguamento rispetto a chi lo ha del tutto eluso)

d) verificare lo "storico" e la situazione concreta dei rapporti tra l'Associazione e i soci e i terzi. Maggiore attenzione va data quando vi siano stati già dei casi di violazione della privacy con danno a terzi oppure lamentele dei soci o situazione di conflittualità interna

d) verificare che nelle **polizze assicurative di RC verso terzi** sia espressamente prevista (e comunque non esclusa) la responsabilità dell'associazione per danni causati a terzi dai propri amministratori e associati, per effetto di un'attività di trattamento posta in essere in violazione del GDPR e in generale della normativa europea e nazionale sul trattamento dei dati personali

27. IL GDPR si applica anche ai trattamenti svolti extra UE? A quali condizioni è ammesso il trasferimento di dati personali all'esterno e in paesi extra UE?

Quando all'ambito di applicazione del GDPR, va detto che ai sensi dell'art. 3 del GDPR le norme del GDPR si applicano:

a) ai trattamenti di dati svolti da un Titolare in un suo "**stabilimento**" (e cioè una organizzazione stabile) che si trova **in un paese UE** (ipotesi che ovviamente riguarda **tutte le ODV, APS e ETS con sede in Italia**, e ciò **anche con riferimento a trattamenti di dati di persone residenti extra UE che vengono trasmessi in Italia e qui utilizzati** (es. associazioni che fanno adozioni a distanza)
b) ai trattamenti di dati svolti da un Titolare anche **in un paese extra UE** quanto quei trattamenti sono però inscindibilmente connessi all'attività svolta dallo stesso Titolare in uno stabilimento che ha sede nella UE
c) al trattamento dei dati svolti da un Titolare anche privo di alcun stabilimento nella UE, quando discende dalla fornitura di un bene o di un servizio (anche gratuita) a **interessati che si trovano nella UE** oppure quando tale trattamento consiste nel **monitoraggio di comportamenti** degli interessati posti in essere nel territorio UE. *Tali principi fanno ad esempio ritenere che siano disciplinati dal GDPR l'offerta di servizi tramite sito internet da parte di una società extra UE e con server extra UE quando il sito utilizza la lingua italiana, un dominio riferito ad uno Stato UE (es. ".it") e prevede delle sezioni specificamente dedicate a cittadini UE.*

Altro aspetto, regolato dagli artt. 44 e seg. del GDPR, riguarda invece le condizioni e i limiti entro cui i Titolari (assoggettati alle regole del GDPR) possano **trasferire dati personali al di fuori dello Spazio Economico Europeo**.

*Il tema è molto "caldo", soprattutto in relazione ai servizi di **Cloud** computing (Google Drive, iCloud Apple, Dropbox) che, **in caso di allocazione del server o dello spazio informatico del cloud in territorio extra UE, comportano un vero e proprio trasferimento di dati extra UE** (oltretutto molto spesso il cliente del servizio cloud non è in grado di sapere dove i suoi dati vengono conservati o trasferiti).*
La scelta del servizio di cloud dovrebbe quindi avvenire previa verifica:
a) che la società estera abbia uno stabilimento nella UE e allochi i dati presso server situati in quello stabilimento (il trasferimento dei dati sul cloud non costituirà allora un trasferimento all'estero e il trattamento sarà assoggettata alle norme del GDPR);
*b) ove invece vi sia un vero e proprio trasferimento extra UE, che la ditta offra garanzie di sicurezza adeguate e in linea con le disposizioni del GDPR, ad evitare i rischi di accesso non autorizzato o perdita dei dati personali. La soluzione migliore, avvalorata anche dall'European Data Protection Board, è quella che la ditta di cloud venga nominata dal Titolare (italiano) **Responsabile (esterno) del trattamento** dei dati trasferiti sul cloud, in una lettera di incarico nella quale la ditta confermi l'esitanza di misure di protezione dei dati adeguate.*
In tema si veda anche il Vademecum edito dal Garante nel 2012 reperibile sul sito www.garanteprivacy.it

Il vecchio Codice italiano prevedeva (art. 43) che il trasferimento di dati all'Estero potesse avvenire solo se l'interessato aveva manifestato il suo consenso in forma scritta.

Ora, l'art. 45 GDPR prevede che **il trasferimento di dati extra UE sia possibile anche senza autorizzazioni o consenso, ove la Commissione Europea abbia verificato che il Paese di destinazione "garantisce un livello di protezione adeguato**" (e ciò sulla base di criteri come l'esistenza di una legislazione ad hoc, la presenza di una Autorità di controllo indipendente, l'adesione a convenzioni internazionali in materia, ecc.) e quindi abbia adottato una DECISIONE DI ADEGUATEZZA. Attualmente sono "coperti" da una decisione di adeguatezza, ad

esempio, l'Argentina, l'Australia, il Canada, Israele, la Nuova Zelanda, la Svizzera e gli **Stati Uniti** (con il cd. *Privacy Shield*).

Inoltre, a prescindere dall'esistenza di una valutazione di adeguatezza, il trasferimento è ritenuto possibile (art. 46 GDPR) qualora vi siano garanzie adeguate per effetto di accordi internazionali, o per l'effetto dell'inserimento nei contratti transfrontalieri di clausole contrattuali "tipo" adottate dalla Commissione o per effetto dell'adesione a codici di condotta o meccanismi di certificazione.

28. Cambia qualcosa se l'ETS ha rapporti con la pubblica amministrazione?

Molte associazioni ed ETS, nello svolgimento dell'attività istituzionale, instaurano rapporti con la Pubblica Amministrazione (es. convenzione, accreditamento, stretta collaborazione all'interno delle strutture sanitarie o socio/assistenziali) ed in ragione di questi rapporti trattano dati personali forniti dagli enti e strutture pubbliche, condividono banche dati o trasmettono alle Pubbliche Amministrazioni i dati dei beneficiari del servizio.

Non è questa la sede per affrontare il complesso e ampio tema del trattamento dei dati personali da parte degli Enti Pubblici. Basti precisare che le Amministrazioni Pubbliche possono trattare:

→ dati personali COMUNI (condizione di liceità del trattamento ex art. 6 comma 1 lett. e GDPR) solo quando il trattamento "*è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*" e solo se (base giuridica del trattamento ex art. 6 comma 3 GDPR) tale compito e tali poteri siano previsto dal diritto dell'Unione Europea o dal diritto italiano;

→ dati personali PARTICOLARI (ex sensibili) solo quando il trattamento "*è necessario per motivi di interesse pubblico rilevante*" sulla base del diritto dell'Unione Europea o del diritto italiano, e in ogni caso tale trattamento "*deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi delle persone*" (art. 9 comma 2 lett. g GDPR). Il Codice italiano (D.Lgs. n. 196/2003 aggiornato al GDPR) ha specificato all'art. 2 sexies in quali casi sussistono i **motivi di interesse pubblico rilevante**, comprendendovi in sostanza tutti gli ambiti di attività delle Pubbliche Amministrazioni. È espressamente previsto che si considera **rilevante l'interesse pubblico quando l'azione della P.A. si svolge nell'ambito dei "*rapporti tra i soggetti pubblici e gli enti del terzo settore*"** (art. 2 sexies comma 2 lett. o del D.Lgs. n. 196/2003), come ad esempio l'elargizione di contributi finalizzati al sostegno degli ETS, la tenuta di registri generali delle medesime organizzazioni e la cooperazione internazionale.

Ciò posto, il GDPR e il Codice italiano non prevedono alcuna espressa eccezione alle norme e ai principi generali (es. sul consenso e informativa, sui Registri del trattamento, sulle misure di sicurezza, ecc.) se il trattamento è svolto da una associazione nell'ambito di un rapporto con la P.A.

Viene però da chiedersi se i particolari trattamenti che riguardano l'attività in convenzione o in accreditamento devono seguire le norme del codice riferite ai soggetti privati (le associazioni sono enti privati), oppure se devono seguire le regole dettate dal GDPR e dal Codice per i "soggetti pubblici", perché anche l'ETS si dovrebbe considerare "soggetto pubblico" quando esegue un "compito di interesse pubblico", e cioè una attività strumentale e/o finalizzata al conseguimento delle finalità pubbliche dell'amministrazione con cui collabora.

Il tema non è semplice. Tendenzialmente si può dire che la stipula di una convenzione non modifica la natura giuridica dell'ODV, APS o associazione, che rimane ente privato. Quando l'associazione tratta i dati personali nella sua struttura, con suoi operatori/Incaricati, con autonomia sotto il profilo gestionale e della privacy, la sua considerazione quale "soggetto pubblico" sarà assai improbabile ed essa dovrà adempiere a tutte le norme riferite ai soggetti privati.

Piuttosto, se il trattamento dei dati è svolto dall'associazione esclusivamente nell'ambito della struttura pubblica e secondo le direttive della P.A., ma anche **quando l'attività di trattamento dei dati da parte dell'associazione è svolta "per conto" della Pubblica Amministrazione Titolare dei dati e per il perseguimento delle finalità proprie della P.A. o stabilite dalla P.A.** (es. dati di cittadini o di persone raccolti dalla P.A. e trasferiti all'ente no profit ai fini dell'esecuzione di un servizio di interesse generale assegnato all'ente no profit quale soggetto convenzionato o accreditato o quale appaltatore; es. gestione del servizio di accoglienza per rifugiati e richiedenti asilo, gestione del parco comunale, ecc.) **sussistono le condizioni per cui l'ETS sia nominato RESPONSABILE DEL TRATTAMENTO**, il che certamente comporta l'assunzione delle

responsabilità collegate a tale ruolo ma permette all'Associazione di avere istruzioni scritte sulla durata, finalità e modalità del trattamento dei dati (vedi art. 28 comma 3 GDPR).

Si consiglia quindi ad ogni associazione ed ente non profit che gestisca dati forniti da enti pubblici nell'ambito di un rapporto giuridico con tali enti di definire con l'ente pubblico quali ruoli e responsabilità ciò comporta anche sotto il profilo della privacy e, nel dubbio, adottare, anche con riferimento a quel trattamento, tutte le prescrizioni del Codice relative all'informativa, al consenso, alle misure di sicurezza adottate in generale per la sua attività.

29. Possono le ODV e gli ETS utilizzare i numeri e gli indirizzi degli elenchi telefonici per campagne di sensibilizzazione o *fundraising*? Possono utilizzare gli indirizzi e-mail o il fax o gli sms o i social network?

Varie associazioni ed ETS svolgono attività di sensibilizzazione e ricerca fondi inviando **comunicazioni via posta cartacea o sms o mail** o **chiamando al telefono** i possibili donatori privati cittadini, usando dati ritrovati nell'elenco telefonico o in internet o in documenti o elenchi pubblici (es. liste elettorali, albi dei professionisti, siti istituzionali delle Pubbliche Amministrazioni, ecc.), che vengono inseriti nella banca dati dell'associazione.

È consentita questa attività ai sensi del GDPR e del Codice italiano?

Molto spesso si pensa che i dati contenuti negli elenchi telefonici (es. indirizzo dell'abitazione, numero di telefono o di fax o di cellulare, indirizzo mail) o in internet (es. numero di telefono e mail) o in elenchi pubblici siano liberamente utilizzabili per il semplice fatto di essere liberamente accessibili e quindi a disposizione di tutti. In realtà ciò non è vero.

La materia era regolata dall'art. 24 del Codice italiano (D.Lgs. n. 196/2003), ora abrogato, secondo erano utilizzabili senza previo consenso dell'interessato i dati "*provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati*". Il Garante aveva tuttavia precisato che l'utilizzo e trattamento di tali dati accessibili a tutti deve avvenire solo se le finalità del trattamento (es. marketing) è compatibile con le finalità che giustificano la presenza dei dati sulla fonte pubblica.

Tale principio è stato sostanzialmente ribadito dal GDPR all'art. 6 comma 4, secondo cui **un trattamento svolto con una finalità diversa** (es. marketing) **da quella per la quale i dati personali sono stati raccolti può avvenire senza il consenso dell'interessato solo se "*il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti*"** (valutazione che spetta al Titolare che vuole svolgere l'attività diversa).

La valutazione di compatibilità di cui sopra porta tendenzialmente ad escludere che per campagne di raccolta fondi e sensibilizzazione possano essere liberamente utilizzati senza previo consenso i dati presenti in internet o nei social network (es. LinkedIn e Facebook) **o in documenti o Albi pubblici** (es. albi dei professionisti, i siti istituzionali delle Pubbliche Amministrazioni, P.R.A.), **perché le finalità per cui tali dati sono pubblici o sono stati resi pubblici** (es. visibilità dell'azienda e dei suoi dipendenti che hanno contatti con il pubblico, comunicazione interpersonale, ricerca del professionista, indicazione dei dipendenti che all'interno di una Pubblica Amministrazione svolgono le funzioni e attività pubbliche, ricerca dei proprietari di autoveicoli) **sono incompatibili con lo scopo dell'attività di marketing o fund raising**. L'associazione dovrà pertanto chiedere il **previo consenso all'interessato**.

*Diverso discorso potrebbe riguardare i dati personali contenuti nei cd. **elenchi categorici** (es. pagine gialle, pagine utili), che hanno natura commerciale e sono utilizzabili per scopi diversi dalla comunicazione personale e quindi forse anche per iniziative commerciali e non profit, senza dover richiedere un previo consenso (ma dovendo comunque trasmettere/comunicare l'informativa); come forse gli indirizzi mail delle persone giuridiche, liberamente utilizzabili in quanto il GDPR si propone di tutelare le sole persone fisiche in relazione al trattamento di loro dati.*

Il Codice italiano (D.Lgs. n. 196/2003 aggiornato al GDPR dal D.Lgs. n. 101/2008) prevede specificamente che:

→ all'art. 129, che il Garante prescriva con apposite Linee Guida le modalità con cui i soggetti che chiedono o consentono alla pubblicazione dei loro dati in "*elenchi cartacei o elettronici a disposizione del pubblico*" prestino il loro **consenso specifico e espresso** all'utilizzo dei loro dati per "*invio di materiale pubblicitario o di vendita diretta o per il perseguimento di ricerche di mercato o di comunicazione commerciale*" (art. 129)

→ all'art. 130 comma 1 e 2, che il consenso è sempre necessario (c.d. **opt-in**) per l'attività di **spam**, e cioè quando le attività di cui sopra vengono svolte con "*sistemi automatizzati di chiamata senza l'intervento di un operatore*" (es. sms o mail-newsletter commerciali)

→ all'art. 130 comma 3 bis, che l'attività cd. di **spam "leggero"** e cioè quella svolta solo attraverso le **chiamate telefoniche** e la **posta cartacea** è consentita anche senza previo consenso (cd. **opt-out**) a meno che la persona destinataria non abbia esercitato il **diritto di opposizione** mediante l'iscrizione nei cd. Registri pubblici delle opposizioni.
Il registro delle opposizioni è stato previsto e regolato in Italia con D.P.R. 178 del 7.9.2010 e con successivo D.P.R. n. 149/2018 e risulta alla pagina web ***www.registrodelleopposizioni.it***. Consente per il momento di bloccare lo spam "leggero" effettuato ai numeri di telefono e agli indirizzi risultanti dagli **elenchi telefonici pubblici** (es. paginebianche). Con L. n. 5/2018 è stata prevista, e sarà attiva dall'1.12.2020, anche l'istituzione di un Registro delle opposizioni riferito all'utilizzo dei **numeri di cellulare** e a tutti i numeri riservati non presenti negli elenchi telefonici pubblici.

Quindi **le Associazioni e gli ETS**, previa istanza rivolta al Gestore del Registro Pubblico delle Opposizioni, **possono contattare telefonicamente o spedire posta cartacea, per raccolta fondi o sensibilizzazione, ai numeri di telefono e agli indirizzi risultanti dagli elenchi telefonici pubblici, ove le persone contattate o i destinatari non siano presenti nel Registro delle opposizioni.**

Va infine segnalato:

→ che le campagne di sensibilizzazione e raccolta fondi possono essere svolte dalle ODV e dagli ETS che svolgono attività a beneficio di terzi utilizzando i **dati presenti nelle LISTE ELETTORALI**. Invero, ai sensi dell'art. 51 D.P.R. n. 223/1967 (norma non espressamente abrogata dal D.Lgs. n. 101/2018, che ha solo abrogato l'art. 177 del D.Lgs. n. 193/2006 che introduceva nel D.P.R. n. 223/1967 il citato art. 51) i Comuni possono rilasciare in copia le liste elettorali se tali liste vengono utilizzate per il "perseguimento di un interesse collettivo o diffuso" (e il Garante, in una decisione risalente al 2005, ha precisato che il perseguimento di tali interessi è tipico degli enti no profit)

→ che i **dati di soci/aderenti** possono essere utilizzati per inviare campagne di sensibilizzazione se tra scopi statutari vi sia anche la propaganda o sensibilizzazione

→ richiede un esplicito previo consenso anche il c.d. **social spam** (invio di pubblicità attraverso messaggi e link nei social network): il Garante ha infatti precisato che non comporta autorizzazione all'invio di messaggi commerciali il fatto che l'utente abbia visitato o si sia iscritto ad un sito sia diventato fan o follower nel social network, a meno che "*dal contesto o dalle modalità di funzionamento del social network, anche sulla base delle informazioni fornite, poteva evincersi in modo inequivocabile che l'interessato avesse in tal modo voluto manifestare anche la volontà di fornire il proprio consenso alla ricezione di messaggi promozionali da parte di quella determinata impresa*".

Quindi si consiglia di inviare mail contenenti campagne di sensibilizzazione e fund raising a coloro che, senza essere soci, si sono iscritti alla newsletter della propria Associazione solo ove nel sito o nel modulo di richiesta (e nell'informativa) sia esplicitato che l'iscrizione comporta anche l'invio di comunicazioni di tale natura.

30. Gli ETS possono pubblicare immagini e video di persone fisiche nel proprio giornalino, nel proprio sito internet o blog o nei propri social network?

Anche le **immagini** sono a tutti gli effetti **dati personali** (comuni), ovviamente ove consentono di riconoscere una persona determinata. L'uso e la pubblicazione delle foto o di video è regolato da varie norme di legge, ed in particolare:

→ l'art. 10 del Codice civile vieta di pubblicare la foto al di fuori dei casi previsti dalla legge e comunque quando la pubblicazione crea un "pregiudizio al decoro o alla reputazione della persona"

→ la legge sul diritto d'autore (n. 633/1941) dice che l'uso del "ritratto" è consentito solo con il consenso della persona oppure quando la riproduzione dell'immagine "è giustificata … da scopi scientifici, didattici o culturali" o "è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico".

Regola generale è quindi quella secondo cui **è necessario chiedere il consenso dell'interessato** all'utilizzo delle sue immagini tramite foto o riprese video, soprattutto se comprende la pubblicazione nel sito internet o nei social network dell'Associazione, che hanno una accessibilità generale e indiscriminata e rispetto ad una

pubblicazione cartacea (es. vecchio giornalino dell'Associazione) aumentano a dismisura la possibilità di estrapolazione e utilizzo indiscriminato delle immagini e dei video, compromettendo la reale possibilità dell'interessato di "seguire" le sorti della loro pubblicazione.

Quindi è necessaria apposita **autorizzazione/liberatoria**:

→ quando ad es. l'Associazione vuole pubblicare sul sito internet o sul giornalino la foto individuale di tutti i soci o la foto di gruppo di tutti i soci, durante il servizio istituzionale o in occasione di eventi "privati" dell'Associazione (assemblee, riunioni associative, gite, seminari ecc.), trattandosi di operazione non strettamente funzionale alla gestione del rapporto associativo

In questo caso la richiesta di consenso al trattamento delle foto/video può essere inserita una volta per tutte nella **MOD. 1 e 2_DOMANDA DI AMMISSIONE A SOCIO**.

→ quando ad es. l'Associazione vuole pubblicare sul sito internet o sul giornalino foto dei beneficiari dell'attività istituzionale, trattandosi di operazione non funzionale al servizio che viene svolto.

In questo caso, considerato che la ripresa foto/video dei beneficiari/utenti non è così frequente, una preventiva richiesta generale deve considerarsi ultronea. Si consiglia quindi di utilizzare una liberatoria da far sottoscrivere solo ai beneficiari presenti in quel momento/giornata scelta per il servizio fotografico o video **MOD. 19_LIBERATORIA IMMAGINI / VIDEO**

→ quando ad es. l'Associazione vuole pubblicare sul sito internet o sul giornalino foto dei partecipanti (non soci) ad un evento (es. convegno, seminario, gita, ecc.).

In questo caso, si consiglia, prima dell'inizio, di **chiedere pubblicamente** e a voce alta ai presenti in sala se qualcuno è contrario alle riprese video/foto, invitando gli eventuali contrari a posizionarsi in una zona dove non saranno ripresi/fotografati. In alternativa, si consiglia di esporre all'ingrasso una **MOD. 5_INFORMATIVA PARTECIPAZIONE EVENTO CON FOGLIO PRESENZE E CONSENSO**, facendo firmare nel foglio presenze il consenso al trattamento delle immagini. Quando l'evento ha una chiara finalità o rilevanza pubblica, potrebbe ritenersi sufficiente e/o consigliato affiggere all'ingresso un **MOD. 18_AVVISO PUBBLICO SU FOTO O VIDEO** con una breve informativa sul fatto che l'Associazione scatterà foto o riprese ad esclusiva descrizione dell'evento, che occasionalmente potrebbero includere anche le persone partecipanti, precisando dove le foto o video verranno pubblicati.

Il consenso non è invece necessario:

→ quando le persone sono **non riconoscibili** perché fotografate o riprese da tergo o solo in parte, oppure in controluce o sfuocate o in lontananza
→ quando le immagini sono acquisite per descrivere e documentare un **evento chiaramente pubblico** (es. sagra del paese, fiera, spettacolo o manifestazione, mostra, ecc.; tipici sono gli eventi organizzati in luogo pubblico da Associazioni Pro Loco) **o un luogo pubblico** (scenari naturali o architettonici) **a condizione che l'obiettivo principale della foto o della ripresa sia appunto la descrizione dell'evento o fatto pubblico o del luogo pubblico in se stesso** (tale che i partecipanti rimangano sullo sfondo o siano ripresi come pubblico indistinto, seppur riconoscibili) e non la ripresa singola in primo piano di uno o più partecipanti.

Si consiglia in ogni caso, in base alla situazione e al buon senso:

→ in un evento pubblico a cui partecipa l'Associazione, non riprendere in primo piano le persone individualmente senza il loro consenso, e comunque utilizzare fotografie che facciano ben intendere il **contesto** nel quale sono collocate le persone (eventi pubblici, aperti al pubblico, eventi culturali)
→ fotografare o riprendere il pubblico tendenzialmente dal retro/**di spalle**/dall'alto o in foto di gruppo a bassa definizione, che non possono essere scaricate e salvate
→ evitare in ogni caso la pubblicazione/diffusione di immagini o video di **minori di 18 anni,** o comunque procedere solo una volta acquisito previamente il consenso scritto dei genitori (o di almeno uno dei genitori, con l'accortezza che egli dichiari di poter firmare da solo in base ai principi sulla responsabilità genitoriale), specificando chiaramente dove le foto o video verranno pubblicati

ATTENZIONE: va prestata attenzione alla **catalogazione dei dinieghi** alla pubblicazione e al rispetto della volontà espressa dagli interessati. Infatti, se la pubblicazione della foto o video di persona non interpellata può essere tutto sommato scusata dalla persona stessa, più ostico potrebbe essere per l'Associazione giustificare

una pubblicazione avvenuta nonostante la persona (es. socio) sia stata previamente coinvolta e abbia negato il consenso alla diffusione.

Ovviamente esulano dalla responsabilità dell'Associazione **le immagini e i video diffusi o postati dai singoli partecipanti o dai soci nei propri canali personali,** sia perché in tal caso l'uso dell'immagine può maggiormente rientrare nella sfera personale e domestica**,** sia perché il mezzo di diffusione non è comunque riconducibile all'Associazione medesima.

Ecco i MODELLI sopra richiamati in cui è riportata la richiesta di consenso all'uso di immagini/video:
1. DOMANDA DI AMMISSIONE A SOCIO CON INFORMATIVA E CONSENSO
2. DOMANDA DI AMMISSIONE A SOCIO MINORENNE CON INFORMATIVA E CONSENSO
5. INFORMATIVA PARTECIPAZIONE EVENTO CON FOGLIO PRESENZE E CONSENSO
18. AVVISO PUBBLICO SU FOTO O VIDEO
19. LIBERATORIA PER FOTO/VIDEO
da utilizzare, integrare e modificare in relazione alla specifica realtà associativa