CENTRO DI SERVIZIO
PER IL VOLONTARIATO
DI VERONA

COMPETENZA E INNOVAZIONE
NEL TERZO SETTORE

AVV. DAVIDE CESTER

LA TUTELA DEI DATI PERSONALI AGGIORNATA AL GDPR NELLE ASSOCIAZIONI DI VOLONTARIATO E NEGLI ENTI DEL TERZO SETTORE

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, usando attenzione e scrupolo, 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 le "dimensioni" del Titolare del trattamento (commisurata ad esempio al numero di lavoratori o volontari) 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 le norme del Regolamento dovranno essere integrate, aggiornate o completate da ulteriori provvedimenti (il Decreto Legislativo italiano di recepimento del Regolamento, che risulta ancora in itinere; i provvedimenti del Garante, i pareri del Comitato Europeo, ecc.) e quindi il

quadro attuale è destinato a cambiare rapidamente e ad evolversi costantemente.
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.

L'Autore

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 primo lavoro.

L'attuale assenza, al momento della stampa del presente manuale, del Decreto Legislativo italiano di recepimento del Regolamento e di tutti i provvedimenti attuativi e di dettaglio rende la materia assolutamente provvisoria e di interpretazione e applicazione non sempre certa.

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 e quale pubblicazione nel sito del Centro di Servizio per il Volontariato della Provincia di Padova *www.csvpadova.org* e di Sardegna *www.sardegnasolidale.it*, ove si potranno reperire i successivi **aggiornamenti** e i **modelli di documenti** da applicare e adattare alla propria realtà associativa.

ATTENZIONE

modelli dei documenti presenti online) solo dopo aver opportunamente "affrontato" quelle precedenti (es. le domande/risposte di spiegazione).

Padova, 5 luglio 2018

Davide Cester, avvocato 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 Treviso, Vicenza e Rovigo.
Ha già pubblicato per il mondo del terzo settore, in ambito privacy, "La privacy nelle associazioni di volontariato e non profit" (Elementi, 2009).
Svolge l'incarico di Data Protection Officer (DPO) in pubbliche amministrazioni ed enti privati.

BOTTA E RISPOSTA: I QUESITI PIÙ IMPORTANTI

Si riportano qui di seguito 25 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? Esiste ancora la "vecchia" privacy?

Il nuovo Regolamento UE del Parlamento e del Consiglio Europeo 2016/679 detto "**General Data Protection Regulation**" (in breve "**GDPR**") segna una ulteriore accelerazione nel campo della riservatezza e del trattamento dei dati personali.
Con la definitiva esplosione dei social network, delle piattaforme informatiche 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 della Regolamento è disponibile nel sito del Garante per la Protezione dei Dati Personali *www.garanteprivacy.it***.**
Al momento, il GDPR non ha comportato l'abrogazione dell'attuale normativa italiana ("Codice in materia di protezione dei dati personali" di cui al D.Lgs. n. 196/2003), la quale resta applicabile in tutte le norme non incompatibili con il GDPR. Sarà il legislatore italiano, in sede di emissione del Decreto Legislativo di "ratifica" del Regolamento UE, a stabilire le sorti della normativa interna (con ogni probabilità verrà abrogata quella parte di disciplina italiana sostituita dal GDPR e verranno conservati o aggiornati gli articoli di dettaglio riferiti a trattamenti particolari di dati per i quali il GDPR prevede la possibilità degli 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 (D.Lgs. n. 196/2003).

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»).

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 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 (ESTERNO) DEL TRATTAMENTO 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: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. In base alle previsioni contenute nella bozza in corso di approvazione del Decreto legislativo italiano di recepimento del GDPR, sembrerebbe che il temine Incaricati vada sostituito con "**PERSONE AUTORIZZATE AL 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:

a) che i dati personali 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) che i dati conosciuti da estranei, che non vengano diffusi **o comunque utilizzati contro la volontà o nell'ignoranza della persona cui si riferiscono**;
c) che i dati personali non vengano distrutti o perduti.

4. Quali dati trattano le ODV ed in generale gli Enti del Terzo Settore e che natura hanno?

Le ODV e APS e in genere gli ETS raccolgono e utilizzano comunemente, nello svolgimento della loro attività, dati personali, e cioè informazioni e notizie riferite:

a) ai propri soci/aderenti;

b) ai beneficiari dell'attività istituzionale o utenti del servizio;
c) ai consulenti e collaboratori esterni;
d) agli eventuali dipendenti;
e) agli enti pubblici;
f) agli altri ETS e in genere i soggetti con cui vengono a contatto;
g) alle persone, enti e aziende a cui indirizzare campagne di sensibilizzazione e *fundraising*, ecc.

*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 possono anche essere gestiti tramite computer e contenuti in **banche dati**, situazione che richiede l'adozione di particolari misure di sicurezza e di protezione dei computer.*

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'avvenuto versamento della quota associativa, gli studi compiuti), alcuni dei quali sono PUBBLICI, e cioè ricavati o comunque ricavabili da albi, elenchi e registri che per legge sono pubblici (es. il codice fiscale o le liste elettorali).

→ **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 una persona determinata. Anche a tali dati, quindi si applicano le regole del GDPR, oltre alle norme del codice civile (art. 10) sulla tutela dell'immagine.

5. Il GDPR riguarda anche le ODV e gli ETS? Si devono considerare "titolari del trattamento"?

Assolutamente SI, buona parte delle norme del GDPR si applicano anche alle ODV e APS ed in generale agli Enti del Terzo Settore, che sono "titolari del trattamento" se e ogni qualvolta svolgono anche una sola delle operazioni che concretano un trattamento di dati personali.

Il GDPR, infatti, non si applica ai 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) e sempre che non si svolga una comunicazione sistematica o diffusione. Il trattamento di dati svolto da una ODV o comunque da un ETS non ha fini esclusivamente personali, comporta molte volte una comunicazione sistematica, 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 e le fondazioni.

Titolare del trattamento è la persona giuridica (qual è l'associazione), nel suo complesso, e non le persone fisiche che ne fanno parte.

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, 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 dell'associazione utilizzi dati personali;
- che, infine, le responsabilità civili, amministrative e penali in caso di violazione del RGDP gravano prevalentemente sulle persone fisiche che hanno agito.

È utile precisare che, ai fini dell'applicazione del Regolamento, non è rilevante l'iscrizione dell'associazione al registro del volontariato ex L. 266/91 o al registro della promozione sociale ex L. 383/00 né al RUNTS di prossima costituzione in base al Codice del Terzo Settore: le norme del GDPR che si riferiscono alle associazioni e agli ETS, infatti, non distinguono tra i vari soggetti appartenenti al terzo settore, ma parlano genericamente di fondazioni, associazioni o organismi senza scopo di lucro.

Posto che per il GDPR il Titolare 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 appunto eserciti un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento.

Se quindi la sezione/organismo locale di una associazione nazionale decide in autonomia in tema di privacy rispetto alla "casa madre", va considerata "titolare", e cioè soggetto autonomo ai fini dell'applicazione del GDPR e del rispetto degli obblighi conseguenti: deve pertanto predisporre una propria informativa, deve chiedere il consenso al trattamento, deve tenere se del caso i Registri del Trattamento e così via.

6. Quali sono i criteri, i limiti e le finalità con cui le associazioni 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 generalmente coincidono o sono compresi negli **scopi istituzionali indicati nello statuto** (anche se spesso lo statuto è spesso generico, ed invece le finalità del trattamento vanno maggiormente 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 e/o l'informazione 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 pubblicità, iniziative commerciali o comunque per scopi che non riguardano l'ente.*

7. Le ODV, APS ed ETS devono fornire all'interessato l'informativa? Le informative redatte in base all'art. 13 del Codice italiano sono sufficienti per il rispetto del GDPR?

Permane anche in base al GDPR, l'obbligo delle ODV, APS ed ETS in generale di fornire l'informativa all'interessato.

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.

Le informative redatte e trasmesse in base al Codice italiano (art. 13 D.Lgs. n. 196/2003) **vanno dal 25 maggio 2018 integrate in base al contenuto dell'informativa descritto all'art. 13 del GDPR e ritrasmesse agli interessati**.

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 sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del **diritto di**

revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

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, paragrafi 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.

L'informativa può essere anche **orale**; tuttavia, poiché il titolare dovrà comunque dimostrare di averla fornita, è evidente che una qualche **forma scritta** è consigliabile.

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

- *per quanto riguarda i **nuovi soci**, l'informativa può **essere allegata o scritta sulla domanda di adesione all'associazione**. Se è prevista una firma del modulo da parte dell'aspirante socio, nel modulo medesimo si potrà avvisare che la firma è richiesta e varrà anche come "presa visione" dell'informativa;*

- *l'informativa può essere anche 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.*

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 acquisisce, conserva e utilizza dati personali**, che si possono definire "interessati".

La comunicazione/consegna va fatta nel momento in cui l'interessato fornisce i suoi dati all'associazione: 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.

*Esigenza di molte associazioni (soprattutto quelle con un elevato numero di soci e con un rapido turn-over) è quella di stampare un'unica informativa e renderla pubblica attraverso l'**affissione** nei locali dell'associazione. Si tratta di una scelta non espressamente ammessa dal GDPR, mentre il Codice italiano prevede forme semplificate di informativa solo in casi specifici o in ragione di un apposito provvedimento del Garante. L'affissione può costituire elemento presuntivo da cui desumere che l'informativa è pervenuta agli interessati; tuttavia potrebbe tutt'al più "coprire" alcuni soci (quelli che si recano in sede), ma non i beneficiari ed in genere le persone che non accedono alla sede dell'associazione. **Si sconsiglia** pertanto di adottare questa forma.*

*Si deve ritenere allo stesso modo **non corretto 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).*

*Maggiore idoneità potrebbe avere l'inserimento/pubblicazione dell'informativa **all'interno del giornale/notiziario dell'associazione** (o allegata allo stesso), se fatto pervenire direttamente agli associati. Va precisato che ai sensi dell'art. 13 del GDPR l'informativa andrebbe comunicata/consegnata nel momento appena precedente a quello in cui l'interessato fornisce i suoi dati all'associazione, e che pertanto la pubblicazione nel giornalino potrebbe essere considerata tardiva. Tuttavia, nel caso in cui l'associazione non abbia finora comunicato alcuna informativa, tale modalità potrebbe rappresentare se non altro una "sanatoria" per regolarizzare la situazione.*

ATTENZIONE: all'informativa va accompagnata la **richiesta di autorizzazione/consenso al trattamento dei dati** in tutti i casi in cui questa è da considerarsi obbligatoria.

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

L'**aggiornamento o rettifica dei dati** (art. 16 RGPD) 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 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 all'associazione le variazioni intervenute (es. cambio di indirizzo). 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 RGDP 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 (si tratta di un'esigenza sentita dalle associazioni, che desiderano anche solo conservare traccia di coloro che hanno "transitato" all'interno dell'ente).

Il RGDP, all'art. 9 comma 2 lett. d) consente l'**utilizzo dei dati (sensibili) degli ex soci** anche senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'associazione 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). 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" (es. invio della newsletter, convocazione per gli anniversari, ecc.), e quindi potranno per esempio ridursi al nominativo e all'indirizzo mail.

Quindi:

- **nell'informativa di cui all'art. 13 GDPD andrà 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 (**DIRITTO ALL'OBLIO**);
- 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.

Quello della conservazione dei dati dopo la cessazione del rapporto associativo è 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 di queste associazioni, o in genere ad una associazione, 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** all'associazione o all'ETS, potrebbero considerarsi, ai sensi dell'art. 9 comma 2 lett. d) RGDP, 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 obblighi di legge di conservazione, essi vanno cancellati quando l'attività o il servizio nei loro confronti debba intendersi definitivamente esaurito.

9. 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 utilizza suoi dati personali e di esercitare i suddetti diritti, e anche le ODV, APS ed ETS, quali titolari, potrebbero ricevere tale richiesta**.

La richiesta potrà pervenire tramite lettera raccomandata, fax o posta elettronica: **si consiglia all'associazione di individuare una persona/Incaricato cui attribuire il compito di evaderla**.

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

10. 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 RGDP contiene, all'art. 9, una definizione (più generica) 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 ODV/APS 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 portatori di handicap 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 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**.

11. Le ODV, APS ed ETS devono chiedere il consenso all'interessato per il trattamento dei suoi dati personali "comuni" e "particolari"?

L'acquisizione del consenso dell'interessato, ove non comporti operazioni gravose, **è sempre consigliata**.

Tuttavia, il Codice italiano e anche il GDPR prevedono espressamente, a favore degli Enti non profit, casi in cui il trattamento può essere svolto senza consenso dell'interessato.

Quanto al Codice italiano, si prevede che, negli "enti senza scopo di lucro", il consenso non è necessario per il trattamento di dati comuni e sensibili dei soggetti "che hanno con essi contatti regolari" o degli "aderenti", se il trattamento è necessario "per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto", e se con l'informativa l'ente comunica all'interessato le modalità dell'utilizzo dei dati, e sempre che i dati non siano comunicati all'esterno o diffusi. In sostanza il Codice italiano stabilisce che **se l'ente *non profit* tratta i dati personali comuni e sensibili dei soci per gli scopi statutari e non li comunica a terzi e non li diffonde, non ha l'obbligo di acquisire il consenso/autorizzazione dei soci.**

Questa esenzione deve considerarsi esistente anche in base al GDPR, che, all'art. 9 comma 2 lett. d), **consente all'associazione l'utilizzo dei dati "particolari**" (e a maggior ragione dei dati comuni) **dei "membri", "ex membri" e delle "persone che hanno regolari contatti" con l'ente, anche senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'associazione e con adeguate garanzie** (di protezione dei dati), **con divieto però di comunicazione all'esterno**.

Profilo delicato resta quello di capire, ai fini dell'esonero dal consenso, se tra le persone che hanno "contatti regolari con l'ente" possano essere inclusi i **beneficiari dell'attività** che ricevono dall'associazione un servizio continuativo.

Con riferimento ai beneficiari e comunque ai non soci, possono però applicarsi alle ODV, APS ed ETS anche altre ipotesi di esclusione del consenso previste dal GDPR.

In particolare, ai sensi dell'art. 6 GDPR, **il consenso non è necessario** quando il trattamento dei **dati comuni**:

- 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).

Ai sensi dell'art. 9 GDPR, il consenso non è necessario quando il trattamento dei **dati "particolari"**:

- 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".

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

- ✓ dei dati comuni e sensibili è necessario per l'adempimento degli obblighi nascenti dal **rapporto di lavoro** con i propri dipendenti;
- ✓ consiste nella comunicazione obbligatoria dei dati comuni all'Agenzia delle Entrate;
- ✓ consiste nella 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**;
- ✓ dei dati comuni serve per eseguire un servizio richiesto dal beneficiario (es. richiesta di trasporto o assistenza domiciliare);
- ✓ di dati particolari/sensibili serve per la tutela della vita o incolumità fisica della persona;
- ✓ di dati comuni avviene per campagne di raccolta fondi (fermo restando il diritto dell'interessato di opporsi).

In ragione dell'incertezza sull'applicazione dei casi di esonero del consenso, **si consiglia di chiedere sempre il consenso ai beneficiari dell'attività se si trattano loro dati particolari/sensibili**.

E va comunque tenuto presente:

→ che anche in caso di esonero dal consenso, **va sempre fornita all'interessato l'informativa**, nella quale descrivere specificamente le modalità con cui l'associazione 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**.

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

Ecco le caratteristiche del consenso descritte all'art. 23 del Codice italiano e all'art. 7 del GDPR:

- **espresso**, cioè esplicito e manifestato in modo inequivocabile (non può essere desunto da un comportamento indiretto);
- **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 di prestare il consenso al trattamento dei suoi dati per finalità estranee all'associazione, pena la sua mancata iscrizione);
- **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 di consenso deve essere sempre preceduta/accompagnata dall'informativa.

Quindi:

- *per quanto riguarda i nuovi soci/aderenti**, l'informativa e la richiesta 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 (anche utilizzando una password appositamente comunicata dal titolare), 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 esperto, 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 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 facile 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, 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 GDPR prevede espressamente che il consenso possa essere rilasciato dai minori che abbiano almeno 16 anni, ma, deve ritenersi, solo con riferimento all'"offerta diretta di servizi della società dell'informazione**" (che sono quei servizi definii 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, Facebook, Dropbox, i cloud, ecc.).

La richiesta di autorizzazione/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.

Come visto, non è semplice districarsi tra norme, ipotesi di esclusione, o capire se si sta svolgendo un trattamento di dati sensibili, o se effettivamente si pone in essere una comunicazione o una diffusione di dati e via dicendo. Nel dubbio è preferibile, in caso di incertezza, far sottoscrivere il consenso, sia per i dati comuni che per i dati sensibili, soprattutto nei casi in cui l'associazione ha "fisicamente" la possibilità di far sottoscrivere l'interessato.

13. Le ODV, APS 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 "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".

Sono quindi tenuti alla nomina del DPO solo gli Enti del Terzo Settore che, nello svolgimento della loro attività principale, svolgono un monitoraggio sistematico SU LARGA SCALA dei beneficiari/destinatari della loro attività o compiono un trattamento SU LARGA scala di dati particolari/sensibili o giudiziari.

Per determinare quando un trattamento di dati è svolto "SU LARGA SCALA" si possono usare criteri quantitativi e qualitativi (numero degli interessati, numero di dati, 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, ecc.

Maggiori indicazioni potranno ricavarsi dagli elenchi di soggetti tenuti alla Valutazione d'impatto sulla protezione dei dati (necessaria proprio se il titolare svolge trattamenti di dati SU LARGA SCALA) che il Garante dovrà redigere ai sensi dell'art. 35 comma 4 GDPR.

14. Esiste ancora la figura del "Responsabile del Trattamento" scelto dal Titolare? Come è meglio chiamare ora il Responsabile "interno"?

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. Così in ambito profit sono stati nominati Responsabili 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 stipulato con il Titolare, un trattamento dei dati "per conto" del Titolare**.

Gli interpreti sono concordi nel ritenere che il nuovo "Responsabile del Trattamento" in base al GDPR è **solo quel soggetto esterno** al Titolare del trattamento. Nel caso di ETS potranno quindi essere nominati Responsabili del trattamento il commercialista che segue l'Associazione, oppure la sezione locale priva di reale autonomia nel trattamento dei dati, oppure l'altro ETS appartenente alla stessa "filiera" dell'ETS Titolare che svolge un trattamento corrispondente al suo ruolo e alla sua attività verso il beneficiario della comune attività, ecc.

Ove l'Associazione avesse 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**".

15. Cosa sono i dati giudiziari?

Il Codice italiano ancora in vigore definisce 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 (art. 4, comma 1, lett. e)

*Sono quindi dati giudiziari molte delle 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 altri. Non invece le sentenze e i provvedimenti civili. Possono entrare a contatto con dati giudiziari le associazioni che operano nella realtà carceraria o che accolgono ex-carcerati (al pari delle cooperative sociali) ad esempio nelle ipotesi di "messa alla prova" o utilizzino o conservino dati relativi al passato o presente giudiziario degli aderenti o dei beneficiari.*

Il GDPR regola i dati giudiziari all'art. 10, stabilendo che "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".

Sembrerebbe quindi che il trattamento dei dati giudiziari da parte di privati (quali gli ETS) non possa basarsi, come è avvenuto finora in base all'art. 27 del Codice italiano, su provvedimento del Garante, e cioè sull'**AUTORIZZAZIONE GENERALE n. 7** del 15.12.2016 (*nel sito www.privacy.it nel link "Garante" – "Autorizzazioni o in www.garanteprivacy.it.*) che consentiva il trattamento di dati giudiziari dei soci e dei beneficiari ad 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.

Si consiglia quindi a tutte le Associazioni ed Enti non profit 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 (es. Tribunale, Ministero della Giustizia) 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.

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

Il Codice italiano definisce **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, sono 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, infatti, agli 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:

- l’adozione e il costante aggiornamento di prassi, procedimenti, strumenti tecnici e informatici specifici e prestabiliti, e cioè previsti e posti in essere prima dell’attività di trattamento (cd. **PRIVACY BY DESIGN**);
- che tali accorgimenti siano introdotti quale “impostazione predefinita” del sistema, tale che un trattamento non conforme sia rifiutato dal sistema (cd. **PRIVACY BY DEFAULT**);
- 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**, 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**, la **MINIMIZZAZIONE** e la **CIFRATURA** dei dati personali;
- 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.

17. 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 o **USER-NAME** e di una parola chiave o **PASSWORD**, 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 (il vecchio "**AMMINISTRATORE DI SISTEMA**").

Questa figura era stata prevista dal DPR 318/99, ma non è stata più riproposta nell'attuale Codice italiano (e nemmeno nel GDPR).

*Ciò non toglie che, nei fatti, ci possa essere e anzi sia **altamente 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 del tutto 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.

18. 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 una certa esperienza nel settore informatico e quindi l'intervento di un tecnico (il cd. amministratore di sistema). 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: può l'associazione decidere che, per comodità, la password sia una sola 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**.

Nel caso vi siano più profili di autorizzazione, la situazione sarà quindi la seguente: se il sistema elettronico è una casa, l'incaricato sarà un visitatore che userà le sue credenziali come una chiave che apre solo alcune porte o tutte le porte. Potrà pertanto accedere ad una sola, a varie o a tutte le stanze a seconda

di quello che ha deciso per lui il "padrone di casa" consegnando a lui la chiave; nelle varie stanze potrà essere da solo (se non esistono altre chiavi oltre alla sua che consentono ad altri visitatori di entrare in quella stanza) o trovare altre persone che vi sono entrate con la loro chiave personale, diversa dalla sua e da quella di ciascun altro ma idonea ad aprire quella stessa serratura (ed eventualmente anche altre).

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

La figura dell'Incaricato del Trattamento è obbligatoria in base all'attuale Codice italiano (art. 30), ma non è espressamente prevista dal GDPR, che all'art. 29 fa solo riferimento a "soggetti istruiti" dal titolare del trattamento.

Nella bozza di D.Lgs. di recepimento del GDPR (art. 2 terdecies e art. 14 comma 1 lett. i) sembra però essere stato abbandonato il termine "incaricato", parlandosi invece di "**persona autorizzata**" o "**designata**" al trattamento dei dati personali sotto l'autorità diretta del Titolare.

A parte l'incertezza terminologica, resta la **necessità per l'Associazione titolare nominare come Incaricati o Autorizzati o Designati al trattamento tutti i soggetti che all'interno e per conto dell'Associazione trattano dati personali** (Presidente, consiglieri, Volontari, dipendenti, ecc.).

Oltretutto, il rispetto delle procedure sugli Incaricati/autorizzati stabilite dal Codice italiano garantisce una migliore dimostrazione di aver adottato le MISURE ADEGUATE di trattamento dei dati.

Quindi è utile e anzi necessario continuare a 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 l'ambito del trattamento consentito (in alternativa, il Codice ritiene sia sufficiente la "preposizione scritta dell'incaricato/autorizzato ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima": questa opzione, si capisce, riguarda gli ambiti aziendali, ed è forse poco adattabile alla realtà delle associazioni non profit);
- 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;

- il titolare potrà consegnare all'incaricato/autorizzato una **lettera di incarico** nella quale lo designa come tale, indica che trattamenti egli può svolgere, su che 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". Chiaramente se i profili sono uguali le lettere di incarico potranno avere lo stesso identico contenuto anche se consegnate a diversi soggetti.

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 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").

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

20. 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. Una condotta sicura sarebbe quella di non inserire e non trattate i dati personali dell'associazione nel computer con cui si naviga in rete, in modo da evitare "contaminazioni"

indesiderate. Tale scelta è un rimedio forse un po' troppo drastico e comunque dispendioso, considerato che le associazioni hanno spesso un solo computer con cui gestiscono insieme le banche dati e accedono a internet e alla posta elettronica.

Se quindi il computer o la "rete" di computer dall'associazione viene collegata a internet o ha un programma di posta elettronica e contiene 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. Potrà essere lo stesso soggetto nominato **AMMINISTRATORE DI SISTEMA**.

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.

21. 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;

Come si capisce, la funzione e il contenuto del Registro dei trattamenti sono assimilabili a quelli 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, tale 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 ODV, APS 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**:

- tutti gli ETS con più di 250 dipendenti;

  Non è da escludere a priori, in via cautelativa, che il dato numerico possa riferirsi anche ai volontari, posto che l'obiettivo della norma è agganciare un obbligo alle proporzioni dell'ente in base al numero di persone che vi svolge attività sia essa retribuita, subordinata, autonoma o volontaria/gratuita

- anche gli ETS con meno di 250 dipendenti, se il trattamento da loro effettuato presenta un rischio per i diritti e le libertà dell'interessato e il trattamento è continuativo (non occasionale);

- anche gli ETS con meno di 250 dipendenti, se il trattamento riguarda in tutto o in parte dati "particolari" ("sensibili" e "biomedici") o dati giudiziari relativi a condanne penali o reati.

Nell'incertezza della norma, e in ogni caso in base alla circostanza per cui facilmente i trattamenti e le attività delle ODV coinvolgono diritti fondamentali o dati sensibili, **si consiglia ad ogni Associazione di predisporre il Registro**, anche perché l'omissione a questo obbligo, ove esistente, determina l'applicazione di una sanzione pecuniaria fino a € 10.000.000,00 (!)

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. In attesa di indicazioni del Garante si può prendere a riferimento la previsione del vecchio Disciplinare Tecnico di un aggiornamento annuale o semestrale, salvo che l'Ente non muti significativamente la propria attività e quindi anche i trattamenti dei relativi dati. Tuttavia, c'è da tener presente che 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.

- non è indispensabile abbia "**data certa**", anche se in via cautelativa è certamente buona prassi inviarlo via pec a terzi, affinché sia possibile

risalire con certezza (giuridica) al giorno in cui è stato redatto o aggiornato.

22. 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 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.

23. Cos'è la Valutazione di impatto sulla protezione dei dati?

Si tratta di una procedura che il DGPR prevede (art. 33) come sostitutiva dell'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 del trattamento", "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 la 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 difficilmente 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.

Per determinare quando un trattamento di dati è svolto "SU LARGA SCALA" si possono usare criteri quantitativi e qualitativi (numero degli interessati, numero di dati, 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, ecc.

Maggiori indicazioni potranno ricavarsi dagli elenchi di soggetti tenuti alla Valutazione d'impatto sulla protezione dei dati (che il Garante dovrà redigere ai sensi dell'art. 35 comma 4 GDPR.

24. Cos'è la Valutazione il Data Breach?

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.

25. 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.

Non è possibile in questa sede, e in attesa del Decreto legislativo italiano di recepimento, fornire un quadro definitivo.

Sul piano penale, di competenza di ciascuno Stato membro, attualmente restano applicabili i REATI previsti dal vigente Codice (D.Lgs. n. 196/2003):

- **Trattamento illecito di dati** (art. 167)

reclusione dai 6 ai 18 mesi per chiunque che, al fine di conseguire un proprio profitto o arrecare danno agli altri, svolge un trattamento in violazione degli art. 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, se dal fatto deriva un danno. Reclusione da 6 a 24 mesi se il fatto consiste nella comunicazione o diffusione.

reclusione da 1 a 3 anni per chiunque che, al fine di conseguire un proprio profitto o arrecare danno agli altri, svolge un trattamento in violazione degli art. 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, se dal fatto deriva un danno.

L'ipotesi più rilevante consiste principalmente nell'aver causato un danno all'interessato utilizzando dati personali senza il suo consenso, quando il consenso è necessario, oppure nell'utilizzo illecito di dati sensibili e giudiziari al fine di procurare danno o trarne profitto.

Nella bozza di D.Lgs. di recepimento del GDPR questa ipotesi di reato è conservata solo in relazione ai trattamenti di dati sensibili e giudiziari che si svolgano in contrasto con le prescrizioni ulteriori stabilite dallo stesso D.Lgs. di recepimento (principalmente, quei trattamenti di dati sensibili o giudiziari che non rispettino le "misure di garanzia" del Garante, equiparabili alle vecchie "autorizzazioni").

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

reclusione da sei mesi a tre anni per chiunque, nella notificazione al Garante o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi.

Nella bozza di D.Lgs. di recepimento del GDPR questa ipotesi di reato è sostanzialmente confermata.

- **Misure di sicurezza** (art. 169)

arresto sino a due anni o ammenda da € 10.000 a € 50.000 per chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33. All'autore del reato, il Garante fissa un termine per la regolarizzazione non superiore a sei mesi. In caso di avvenuta

regolarizzazione entro i 60 giorni successivi allo scadere del termine, il Garante ammette il pagamento di € 12.5000, il cui pagamento estingue il reato.

Nella bozza di D.Lgs. di recepimento del GDPR è prevista l'abrogazione dell'art. 169, e ciò in quanto la mancata adozione delle misure di sicurezza (non più minime, ma adeguate) è ora colpita da una grave sanzione pecuniaria in base al GDPR.

Sempre la bozza di D.Lgs. di recepimento prevede, quali nuove ipotesi di reato la "comunicazione o diffusione illecita di dati personali riferibili ad un rilevante numero di persone" (nuovo art. 167bis del Codice), l'"acquisizione fraudolenta di dati personali" (nuovo art. 167ter del Codice).

Le norme penali parlano genericamente di "chiunque", ma i soggetti che rispondono del reato non sono di facile individuazione[1].

Soprattutto, 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 (ad esempio ha deciso che trattamenti svolgere e le loro modalità, o ha deciso che misure adeguate adottare). Quindi i membri del Consiglio Direttivo, il Presidente dell'associazione, il Delegato del trattamento o l'Amministratore di sistema eventualmente nominati sono le figure più "esposte"; il ***Presidente*** *si potrà liberare da responsabilità dimostrando di aver conferito al Delegato (ex 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* ***Delegato*** *o dell'****Amministratore di sistema*** *questa prova liberatoria sarà forse più difficile: egli potrà dimostrare che non gli erano state attribuite quelle funzioni il cui scorretto esercizio ha determinato il compimento di un reato, ma l'esistenza di istruzioni scritte del titolare potrebbero rendere questa prova più ardua. 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.*

La responsabilità penale, comunque, richiede l'esistenza di vari elementi: nel caso dell'art. 167 è richiesto il dolo (cioè la volontà di commettere il reato), nel caso

[1] I commentatori hanno sostenuto, ad esempio: che i reati di inosservanza delle prescrizioni contenute nelle autorizzazioni del Garante al trattamento dei dati sensibili (art. 26, comma 2) e la mancata adozione delle misure minime di sicurezza (art. 33) possono colpire esclusivamente il Titolare (e il Responsabile, se delegato); che il reato della mancata acquisizione del consenso (art. 23) può colpire il titolare ma anche l'incaricato, quando quest'ultimo non ha rispettato le direttive specifiche fornite dal titolare; che il reato di illecito trattamento di dati sensibili (art. 25) può essere compiuto da qualsiasi soggetto.

degli art. 168 e 169 è punita anche la colpa (ovvero la disattenzione, la noncuranza, l'imperizia, ecc.); in alcuni casi è richiesto il fine specifico (es. di arrecare danno o acquisire denaro), in altri che un danno si sia effettivamente verificato. L'accertamento della responsabilità penale comporta un'indagine svolta dal pubblico ministero, che, al termine di essa, chiede al Tribunale la condanna o l'archiviazione. Nel primo caso si svolge il giudizio davanti al Tribunale.

*Ci si può chiedere a questo punto quale sia il **rischio concreto** per le associazioni di volontariato 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 frequente 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** previste dall'art. 83 del GDPR sostituiscono quelle previste dall'attuale Codice italiano.

In sintesi:

- è soggetta alla **sanzione pecuniaria (multa) "fino a € 10.000.000,00**" la violazione 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.

- è soggetta alla **sanzione pecuniaria (multa) "fino a € 20.000.000,00**" ad esempio la violazione:

  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 nelle FAQ 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).

- 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 gravissimo, 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 indica specifici elementi che possono provocare, anche l'applicazione di una sanzione di basso importo** (si noti oltretutto che l'art. 83 non prevede un importo minimo della sanzione, con ciò ammettendo che possa essere anche di € 100,00 o meno), 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 anziché 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

D'altra parte, però, la sanzione va commisurata anche alla categoria di dati personali interessate dalla violazione, e quindi una violazione che riguarda DATI SENSIBILI o GIUDIZIARI può comportare l'applicazione di sanzioni rigorose.

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. 157-160 del Codice), 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. 689/81: 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*[2]*.*

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").

Altro potere del Garante è quello, previsto dall'art. 143 del Codice e 58 del GDPR, di imporre il blocco o la sospensione del trattamento illecito, di prescrivere al titolare l'adozione di idonee misure per renderlo lecito.

L'applicazione delle sanzioni amministrative è condizionata dalla gravità del fatto: se ad esempio la mancata comunicazione dell'informativa è elemento forse decisivo, in un caso di incompletezza della stessa il Garante ha ritenuto che andasse modificata ma non fosse "tale da implicare l'applicazione di una sanzione" (provv. 10.1.2002 in www.privacy.it).

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

L'art. 82 GDPR, infatti, prevede che

> chiunque subisca un danno materiale o immateriale causato dalla violazione del presente Regolamento 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 (da "attività pericolosa"), in quanto:

- deriva dalla mera violazione di una prescrizione del GDPR;

[2] Il procedimento è lo stesso rispetto ad esempio, ad una multa per eccesso di velocità.

- implica l'inversione dell'onere della prova: non è il danneggiato a dover dimostrare che il danno dipende da chi ha trattato i suoi dati, ma **sono il Titolare o il responsabile che, per liberarsi da responsabilità, devono dimostrare "che l'evento dannoso non gli è in alcun modo imputabile**", e cioè, in sostanza, di aver adottato tutte le misure idonee ad evitare il danno" (come prevede il Codice del 2003 facendo riferimento all'art. 2050 c.c.): 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 tecniche, procedimentali e organizzative dirette alla tutela dei diritti dell'interessato.

Quindi se un ODV, un APS o un'ETS violano le norme del Regolamento causando un danno a terze persone, potranno esser chiamate in causa dal danneggiato davanti al giudice civile per ottenere il risarcimento del danno patrimoniale e/o morale. Risponderanno con i beni dell'associazione e anche – se l'associazione non ha la personalità giuridica – con il patrimonio personale delle persone fisiche che hanno agito in nome e per conto dell'Associazione in ambito privacy.

Fino ad ora le pronunce dei Tribunali hanno colpito soprattutto l'illegittima pubblicazione da parte dei giornali (senza preventiva acquisizione del consenso dell'interessato) dell'immagine della persona, o di un indirizzo privato, o del nominativo della vittima di un furto, ritenendo che, nei singoli casi, la pubblicazione non poteva dirsi giustificata dall'esercizio del diritto di cronaca. Si deve pertanto ritenere che qualche pericolo possa derivare alle associazioni, ad esempio, dalla diffusione del proprio giornalino, qualora qualche dato o immagine sia pubblicata senza aver ottenuto il consenso della persona: tuttavia ***l'azione civile presuppone una iniziativa del soggetto danneggiato****, ed è abbastanza improbabile che quindi sia svolta da persone che hanno contatti "amichevoli" con l'associazione.*