Volontarinsieme
CSV Treviso

LA TUTELA DEI DATI PERSONALI NELLE ASSOCIAZIONI DI VOLONTARIATO E PROMOZIONE SOCIALE E NEGLI ENTI DEL TERZO SETTORE

in base al GDPR e al D.Lgs. n. 196/2003
aggiornato con D.Lgs. n. 101/2018

AVV. DAVIDE CESTER

SOMMARIO (edizione del Gennaio 2019)

PRESENTAZIONE ALLA TERZA EDIZIONE

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

L'Autore

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.

IMPORTANTE – ISTRUZIONI PER L'USO

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

ATTENZIONE

Padova, gennaio 2019

BOTTA E RISPOSTA: I QUESITI PIÙ IMPORTANTI

Si riportano qui di seguito 29 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**", pronunciato in inglese "GiDiPiAr") segna una ulteriore accelerazione nel campo della tutela della riservatezza e del trattamento dei dati personali.

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

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

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

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

2. Definizioni vecchie e nuove

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

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

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

INTERESSATO è la persona fisica identificata o identificabile attraverso i suoi dati personali. "Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Non è soggetto "interessato", per il GDPR, la persona giuridica.

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

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

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

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

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

INCARICATI: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. In base alle previsioni contenute nel GDPR e nel Codice italiano (art. 29 GDPR e art. 2 *quaterdecies* del Codice), possono essere definite anche quali "**PERSONE AUTORIZZATE O DESIGNATE 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.
h) agli utenti del proprio **sito** istituzionale.

*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 nella maggior parte dei casi sono però gestiti **in via informatica** e sono contenuti in **banche dati**, in alcuni casi anche mediante sistemi di cloud, situazioni che richiedono l'adozione di particolari misure di sicurezza e di protezione.*

Quanto alla natura dei dati, permane la distinzione tra:

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

Costituiscono dati personali (comuni o sensibili) anche le **IMMAGINI**, i suoni, i video ecc., quando consentono di individuare 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"? Possono essere "contitolari 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 al loro interno anche una sola delle operazioni che concretano un trattamento di dati personali, decidendo la finalità e le modalità del trattamento stesso.

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, impianto di sorveglianza ad uso esclusivamente privato, ecc.) e sempre che non si svolga una comunicazione sistematica o diffusione. Il trattamento di dati svolto da 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 nel suo complesso (e quindi l'Associazione, la Fondazione, il Comitato, ecc.) **e non le persone fisiche che ne fanno parte o che ne hanno la rappresentanza legale**.

Ciò non toglie:
- che le decisioni sui trattamenti da svolgere vanno adottate dall'organo o dalle persone fisiche cui è attribuita la gestione dell'ente (es. Consiglio Direttivo, 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 o hanno omesso di adottare le misure di sicurezza necessarie.

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

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

Quando le decisioni sulle finalità e sui mezzi/modalità del trattamento vengono assunte insieme, gli enti coinvolti si definiscono **CONTITOLARI DEL TRATTAMENTO** e ai sensi dell'art. 26 GDPR devono redigere e sottoscrivere un apposito **ACCORDO DI CONTITOLARITA'**, nel quale descrivere le finalità e modalità dei

trattamenti, i ruoli, i rapporti e le relative responsabilità in relazione agli obblighi derivanti dal GDPR (informative, rapporti con gli interessati, misure di sicurezza informatiche, prassi organizzative comuni o uniformi, ecc.).

6. Quali sono i principi e i limiti con cui 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 tendenzialmente coincidono o sono compresi negli scopi istituzionali indicati nello statuto** (anche se lo statuto è spesso generico, e le finalità del trattamento vanno specificate nell'informativa)

Quindi ad esempio quando l'associazione raccoglie i dati comuni dei suoi associati per inserirli nel libro soci, per inviare a casa la corrispondenza o il giornalino dell'associazione e comunque per averne la reperibilità, o raccoglie i dati dei beneficiari dell'attività per garantire il servizio, ***non potrà senza l'autorizzazione 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 marketing, iniziative commerciali o comunque per scopi che non riguardano l'ente.*

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

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

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

7. Le ODV, APS ed ETS devono fornire all'interessato l'informativa? Con che contenuto e modalità? Le informative trasmesse prima del maggio 2018 in base all'art. 13 del Codice italiano sono ancora idonee?

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

Permane anche in base al GDPR, l'obbligo di fornire l'informativa all'interessato.
Le informative redatte e trasmesse in base al Codice italiano (art. 13 D.Lgs. n. 196/2003) **vanno integrate in base al contenuto dell'informativa descritto all'art. 13 del GDPR e ritrasmesse agli interessati** (salvo ovviamente non presentassero già allora il contenuto ora richiesto dal GDPR).

L'informativa deve contenere:

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

Inoltre, la stessa informativa deve contenere:

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

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

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

- *ai fini probatori, è sempre preferibile, ove si possa incontrare di persona l'interessato, sottoporgli un'informativa scritta;*
- *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 esclusa dal GDPR. L'affissione può certamente costituire elemento presuntivo da cui desumere che l'informativa è pervenuta agli interessati; tuttavia potrebbe tutt'al più "coprire" alcuni soci abituali, ma non i beneficiari ed in genere le persone che non accedono alla sede dell'associazione. **Si sconsiglia** pertanto di adottare solo questa forma di informativa.*

*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. Tuttavia, questa modalità consente di informare solo i soci che ricevono il giornalino, e quindi non copre gli aspiranti soci e i soggetti diversi dai soci (avuto riguardo che ai sensi dell'art. 13 del GDPR l'informativa va comunicata/consegnata nel momento appena precedente a quello in cui l'interessato fornisce i suoi dati all'associazione).*

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

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

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

ATTENZIONE: all'informativa va accompagnata la **richiesta di consenso al trattamento dei dati** in tutti i casi in cui questa è da considerarsi obbligatoria o è consigliata.
Si allegano al presente lavoro i seguenti **ESEMPI E MODELLI DI INFORMATIVA E RELATIVO CONSENSO AL TRATTAMENTO da utilizzare, integrare e modificare in relazione alla specifica realtà associativa**:

1. **INFORMATIVA E CONSENSO per SOCI**
2. **INFORMATIVA E CONSENSO per SOCI MINORENNI**
3. **INFORMATIVA E CONSENSO per BENEFICIARI ED ESTERNI**
4. **INFORMATIVA E CONSENSO per BENEFICIARI ED ESTERNI MINORENNI**
5. **INFORMATIVA per CONSULENTI COLLABORATORI E FORNITORI**
6. **INFORMATIVA E CONSENSO per DIPENDENTI**
7. **INFORMATIVA PER UTENTI SITO INTERNET**
8. **INFORMATIVA PER ISCRITTI ALLA NEWSLETTER**

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 o di indirizzo e-mail). L'aggiornamento/rettifica dei dati è anche un vero e proprio diritto dell'interessato.

Quanto al problema della **conservazione dei dati,** soprattutto alla luce del nuovo 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.

Il RGDP, all'art. 9 comma 2 lett. d) consente l'**utilizzo dei dati (anche sensibili) degli ex soci** 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 va specificato quali dati l'associazione intende conservare anche dopo la cessazione del rapporto associativo,** fermo restando l'avvertimento all'interessato che comunque, in ogni caso, il socio cessato potrà chiederne la cancellazione;
- dei dati del socio cessato è comunque **vietata la comunicazione all'esterno o la diffusione** (salvo esplicito consenso del socio);
- con le opportune cautele per evitarne la diffusione, l'associazione potrà, secondo i principi di cui sopra, conservare una sorta di "**albo d'oro**" con i nominativi di coloro che sono stati soci, attraverso una rubrica o albo cartaceo (o attraverso lo stesso libro soci "storico") conservati in luogo non accessibile a terzi.

La conservazione dei dati degli ex soci è esigenza sentita dalle Associazioni, che desiderano anche solo avere traccia di coloro che hanno "transitato" all'interno dell'ente. Si tratta comunque *di un aspetto comunque delicato, soprattutto con riferimento a quei dati considerati "sensibili", in quanto idonei "a rivelare l'adesione ad associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale". Si capisce che la diffusione o la comunicazione a terzi di una precedente iscrizione ad una 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** di denaro 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 il Titolare utilizza suoi dati personali e di esercitare i suddetti diritti, e anche gli ETS, quali Titolari, potrebbero ricevere tale richiesta**. Le modalità di esercizio di tali diritti devono essere esplicitate nell'informativa (generalmente si indica un indirizzo di posta elettronica o un contatto telefonico o un numero di fax o la lettera raccomandata): **si consiglia all'associazione di individuare una persona/Incaricato cui attribuire il compito di evaderla**.

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

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

Le 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. Sono ancora valide le Autorizzazioni Generali del Garante italiano? Le Associazioni devono chiedere l'autorizzazione al Garante per il trattamento dei dati sensibili?

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

Dopo l'abrogazione degli art. 26 e 40 da parte del decreto di recepimento D.Lgs. n. 101/2018, il Garante, ai sensi dell'art. 21 dello stesso D.Lgs. n. 101/2018, ha individuato, con recentissimo provvedimento del 13.12.2018, le "*prescrizioni contenute nelle autorizzazioni generali già adottate … che risultano* ***compatibili*****" con il GDPR**, avviando una **consultazione pubblica** per ricevere osservazioni o proposte in ordine all'aggiornamento di tali prescrizioni (da far pervenire all'indirizzo *consultazione.prescrizioni@gpdp.it* entro l'11.2.2019).

Tra le autorizzazioni ancora in vigore (in quanto dichiarate dal Garante compatibili con il GDPR) vi è anche appunto la **n. 3/2018**, che il Garante ha aperto alla consultazione in ordine ad aspetti quali:

- ✓ l'individuazione delle **finalità del trattamento dei dati sensibili** svolto dagli ETS (la cui elencazione dovrà presumibilmente tener conto delle nuove previsioni dell'art. 5 e 6 del Codice del Terzo Settore sulle "attività di interesse generale" e sulla "attività diverse" degli ETS);
- ✓ la possibilità delle Associazioni di **comunicare i dati del singolo socio anche agli altri soci** solo se tale possibilità sia prevista dallo statuto, se le modalità di tale comunicazione siano descritte nell'informativa ex art. 13 GDPR, e se vengano comunque rispettati i principi di necessità, finalità e minimizzazione (e venga comunque preferita la comunicazione individuale al socio laddove vengano in considerazione profili esclusivamente personali);
- ✓ la comunicazione e la diffusione dei dati sensibili all'esterno dell'associazione, da svolgersi con il consenso degli interessati, previa informativa e purché i dati siano strettamente pertinenti alle finalità ed agli scopi perseguiti.

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

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

Il GDPR prevede varie ipotesi in cui il trattamento dei dati comuni e sensibili può avvenire anche senza il consenso (art. 6 comma 1 e art. 9 comma 2 GDPR). Si tratta però di ipotesi piuttosto limitate e di non semplice inquadramento, e quindi per l'Associazione **l'acquisizione del consenso** dell'interessato **è sempre consigliata**.

Quanto ai soci, l'art. 9 comma 2 lett. d) del GDPR consente all'associazione l'utilizzo dei **dati sensibili/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 e finalità dell'associazione e con adeguate garanzie (di protezione dei dati), **con divieto però di comunicazione e diffusione all'esterno**.

In termini generali (e quindi con riferimento sia ai soci, sia beneficiari dell'attività sociale, sia ai terzi in generale) 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).

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

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**.

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

Ecco le caratteristiche del consenso descritte all'art. 7 del GDPR:
- **espresso**, cioè esplicito e manifestato in modo inequivocabile (non può essere desunto da un comportamento indiretto o dal silenzio)
- **libero**, cioè manifestato liberamente dal soggetto, richiesto in termini non definitivi e non incondizionati. Inoltre, il consenso non può essere imposto se invece è facoltativo (ad esempio l'Associazione non potrà imporre all'aderente, quale condizione per l'iscrizione a socio, di prestare il consenso al trattamento dei suoi dati per finalità estranee a quelle istituzionali)
- **specifico**, ovvero riferito ad uno o più trattamenti individuati e aventi specifiche finalità, e descritti con linguaggio semplice e chiaro
- **informato**, ovvero preceduto dall'informativa di cui all'art. 13
- **sempre revocabile** (ovviamente la revoca non comporta l'illegittimità dei trattamenti svolti in precedenza).

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

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

Quindi:

- *per quanto riguarda i nuovi soci/aderenti**, l'informativa e la dichiarazione di consenso possono essere allegati o contenuti nella domanda di adesione all'associazione**, o scritti nel retro*
- *la richiesta di consenso può essere anche spedita **via mail**, con la richiesta all'interessato di inviare una mail (non automatica) di "conferma" (che l'ente potrà stampare e conservare), quando però gli sia stato reso chiaramente noto che il messaggio di risposta sarà inteso quale autorizzazione al trattamento*
- *se l'associazione gestisce un sito web esiste la possibilità di utilizzare il cd. **point&click**, ovvero di creare attraverso appositi software una pagina web nella quale l'interessato può accedere per fornire i propri dati personali, per essere informato delle modalità del trattamento, e soprattutto per autorizzare il trattamento barrando una o più caselle (**che non sia già "preflaggate"**). Tale operazione rende molto semplice per le associazioni la raccolta dei dati, la comunicazione dell'informativa e l'acquisizione del consenso e si traduce in un buon risparmio di tempo per chi richiede e fornisce il consenso; importa però una certa spesa e l'intervento di un tecnico informatico, poiché richiede il rispetto di alcuni precisi requisiti di sicurezza e riservatezza delle transazioni informatiche, da valutare a seconda della tipologia dei dati forniti. È pertanto consigliata solo per le grandi associazioni*
- *il consenso va acquisito **una sola volta** se il trattamento dei dati non cambia e rispetta le finalità indicate nell'informativa medesima*
- *il consenso va richiesto **solo a quei soggetti dei quali l'Associazione raccoglie, registra o utilizza i dati**, e tra costoro non rientrano ovviamente i soggetti beneficiari dell'attività istituzionale che l'ente non identifica*
- *se l'associazione ha chiesto e ottenuto il consenso nel vigore del Codice italiano non ha l'obbligo di acquisirlo nuovamente, a meno che i trattamenti che svolge si siano a tal punto modificati da richiedere un'autonoma manifestazione di volontà dell'interessato.*

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

Con riferimento agli interessati che siano **MINORENNI, il consenso va prestato da coloro che esercitano la responsabilità genitoriale** o, se esiste, dal tutore. Il Codice italiano all'art. 2 quinquies consente espressamente che il consenso possa essere rilasciato dai minori che abbiano almeno 14 anni solo con riferimento all'"**offerta diretta di servizi della società dell'informazione**" (che sono quei servizi 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, i social network, i servizi digitali in genere).
*Spesso ci si chiede se il consenso per il trattamento dei dati del figlio minorenne vada sottoscritto da **entrambi i genitori** o sia sufficiente la firma di **uno solo**. Regola generale è quella per cui, a prescindere dallo stato di convivenza, matrimonio, separazione o divorzio, i genitori devono assumere insieme le scelte di "straordinaria amministrazione" (e cioè quelle di maggiore interesse per il minore, attinenti all'istruzione, educazione, salute e residenza abituale), mentre le decisioni ordinarie e quotidiane possono invece essere assunte anche da uno solo dei due genitori. Non è semplice capire se il consenso al trattamento dei dati personali sia una decisione di ordinaria o straordinaria amministrazione, e non è determinante che il GDPR, all'art. 8 comma 2, parli al singolare di "titolare della responsabilità genitoriale". Si consiglia comunque di prestare particolare attenzione alle richieste di consenso ai trattamenti di dati sensibili o che comportano una diffusione dei dati o immagini del figlio. Nel caso in cui non vi sia la possibilità o l'intenzione di acquisire il consenso di entrambi i genitori, può essere utile inserire nella formula del consenso la precisazione per cui la firma dell'unico genitore viene apposta "in conformità alle norme sulla responsabilità genitoriale di cui agli artt. 316, 337 ter e 337 quater del codice civile" (in sostanza, di comune accordo con il genitore che non firma e/o non si rapporta con l'Associazione).*

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

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.

Si allegano al presente lavoro i seguenti **ESEMPI E MODELLI DI INFORMATIVA E RELATIVO CONSENSO AL TRATTAMENTO da utilizzare, integrare e modificare in relazione alla specifica realtà associativa**:

1. **INFORMATIVA E CONSENSO per SOCI**
2. **INFORMATIVA E CONSENSO per SOCI MINORENNI**
3. **INFORMATIVA E CONSENSO per BENEFICIARI ED ESTERNI**
4. **INFORMATIVA E CONSENSO per BENEFICIARI ED ESTERNI MINORENNI**
5. **INFORMATIVA per CONSULENTI COLLABORATORI E FORNITORI**
6. **INFORMATIVA E CONSENSO per DIPENDENTI**
7. **INFORMATIVA per UTENTI SITO INTERNET**
8. **INFORMATIVA per ISCRITTI ALLA NEWSLETTER**

14. 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 2003, del "Responsabile della Protezione dei Dati".

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

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

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

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

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.

Maggiori indicazioni derivano dall'"**Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati**" (valutazione necessaria proprio se il Titolare svolge trattamenti di dati SU LARGA SCALA) pubblicato dal Garante italiano ai sensi dell'art. 35 comma 4 GDPR con provvedimento dell'11.10.2018.

Il Garante ha identificato siano **trattamenti SU LARGA SCALA** ipotesi abbastanza distanti dalla normale attività degli ETS (scoring o profilazione su larga scala e attività predittive relative al rendimento professionale, alla situazione economica, alla salute, alle preferenze o gli interessi personali, all'affidabilità o al comportamento, all'ubicazione o agli spostamenti dell'interessato; screening sulla persona per assumere decisioni rilevanti su di essa; osservazione, monitoraggio o controllo sistematico degli interessati anche attraverso reti e app; trattamenti su larga scala di dati estremamente personali come quelli della vita familiare o privata, l'ubicazione o dati finanziari; controllo a distanza dell'attività di dipendenti; trattamenti che usano tecnologie innovative come sistemi di intelligenza artificiale, scanning vocale e testuale; scambio tra diversi titolari di dati su larga scala con modalità telematiche; interconnessione, combinazione o raffronto di informazioni; trattamenti sistematici di dati biometrici e dati genetici).

Vi sono tuttavia due ipotesi di trattamenti SU LARGA SCALA assai frequenti per gli ETS, ed in particolare:

→ i "**Trattamenti non occasionali di dati relativi a SOGGETTI VULNERABILI (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)**"

→ i "Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse"

Sono quindi tenuti alla nomina del DPO 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 NON OCCASIONALE di dati relativi a SOGGETTI VULNERABILI (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo) o compiono trattamenti SU LARGA scala di dati "particolari" (ex sensibili) o di dati giudiziari interconnessi con altri dati personali raccolti per finalità diverse**.

15. 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. Sono stati così nominati Responsabili del trattamento i dirigenti dei vari settori dell'impresa o le figure apicali degli uffici amministrativi degli enti pubblici o anche qualche membro del Consiglio Direttivo di ODV o APS.

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

Gli interpreti sono concordi nel ritenere che il nuovo "Responsabile del Trattamento" in base al GDPR è solo quel **soggetto esterno** al Titolare che svolge un trattamento per conto e su incarico del Titolare. Nel caso di ETS potranno (rectius, dovranno) quindi essere nominati Responsabili del trattamento la ditta che fornisce l'assistenza informatica, la ditta che svolge compiti amministrativi o contabili, oppure l'altro ETS appartenente alla stessa "filiera" o allo stesso gruppo che svolge, per la "capogruppo" o per gli altri ETS del gruppo, specifici servizi che comportano un trattamento di dati, 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**" (o "Responsabile **interno** del trattamento").

Si allega al presente lavoro un esempio/modello di
9. ATTO DI NOMINA A RESPONSABILE REFERENTE INTERNO
11. ACCORDO/INCARICO AL RESPONSABILE ESTERNO DEL TRATTAMENTO
da utilizzare, integrare e modificare in relazione alla specifica realtà associativa

16. Cosa sono i dati giudiziari? Possono essere trattati dalle ODV?

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

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

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

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

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

In definitiva, il trattamento di dati giudiziari è ora possibile se si rientra nelle ipotesi di liceità dell'art. 6 GDPR (**vedi par. 12**), e se è presente almeno una di queste condizioni:

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

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

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

In ogni caso, e soprattutto al di fuori delle ipotesi sopra indicate, si consiglia a tutte le ODV 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 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.

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

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

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

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

e ciò al fine:

- "di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente" al GDPR
- "di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"

- di assicurare "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico";
- di assicurare "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

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

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

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

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

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

c) ulteriori strumenti e metodi sono indicati all'art. 26 e 32 del GDPR nell'ambito del principio cd. della "PRIVACY BY DEFAULT", e sono:
   - la **PSEUDONIMIZZAZIONE** (conservazione separata dei dati dell'interessato tale che un solo dato non ne consente l'identificazione), la **MINIMIZZAZIONE** (eliminazione dati inutili, generalizzazione dei dati rimasti) e la **CIFRATURA** dei dati personali (trasformazione del dato in una sequenza apparentemente casuale di numeri e lettere e segni che sono riconvertitili nel dato originario solo con apposita chiave);
   - le misure tecniche e organizzative dirette a garantire che, "per impostazione predefinita", siano svolti solo i trattamenti di dati (per quantità di dati, periodo di conservazione e accessibilità) corrispondenti alle specifiche finalità del trattamento;
   - le misure tecniche e organizzative dirette a garantire che, "per impostazione predefinita", non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica;
   - l'adozione di una **PROCEDURA PER TESTARE**, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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

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

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

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

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

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

L'individuazione iniziale delle password e degli *username* è generalmente svolta da un soggetto esterno esperto informatico, che nel passato è stato identificato nell'**Amministratore di Sistema** previsto *dal DPR 318/99, non più previsto nell'attuale Codice italiano (e nemmeno nel GDPR). Ciò non toglie che, nei fatti, ci possa essere e anzi sia* ***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.

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

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

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

La predisposizione di un sistema di autorizzazione è necessaria solo se ci sono più "profili": **il titolare infatti può anche decidere che tutti gli incaricati/autorizzati accedano a tutti gli ambiti del trattamento che si**

svolge nella sua struttura (cioè a tutte le banche dati o a tutti i programmi): in questo caso non sarà necessario un "sistema" perché il profilo di autorizzazione sarà unico (uno stesso profilo per tutti gli incaricati/autorizzati).

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

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

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

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

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

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

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

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

Quindi è utile 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 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 (**vedi par. 19**)
- 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" (**vedi par. 19**). 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").

Si allega al presente lavoro un esempio/modello di **(10.) ATTO DI NOMINA A INCARICATO/AUTORIZZATO AL TRATTAMENTO da utilizzare, integrare e modificare in relazione alla specifica realtà associativa**.

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

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

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

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

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

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

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

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

*sicure. In generale è consigliato rivolgersi ad un **tecnico di fiducia**, con cui iniziare un rapporto di collaborazione, e che curi non solo l'installazione ma anche la manutenzione dei sistemi operativi ed elettronici.*

La difesa da programmi pericolosi e virus si attua anche attraverso altri **accorgimenti e attenzioni** da parte dell'incaricato/utilizzatore del computer, non obbligatorie ma consigliabili, come ad esempio:

- non aprire e-mail o allegati dall'incerta o pericolosa provenienza
- non installare programmi scaricati da siti non ufficiali o comunque di natura incerta
- tenere sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti/programmi; disattivare sul browser l'esecuzione automatica degli script Java e Activex
- eseguire periodicamente la pulizia del disco fisso da "cookies", file temporanei ecc.
- evitare i falsi allarmi e le catene di sant'Antonio, controllando preventivamente la bontà delle informazioni prima di diffonderle.

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

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

In questo caso è importante:

- evitare il più possibile che l'accesso venga svolto mediante **computer di terzi** o comunque sistemi informatici di cui non si possa verificare il sistema di sicurezza e protezione
- **non utilizzare le stesse credenziali** (username e password) **per l'accesso ai diversi servizi online** (es. Posta elettronica dell'Associazione, Facebook, Home banking, Posta elettronica personale, ecc.), in quanto la violazione di uno di questi ambiti potrebbe comportare l'acquisizione da parte di terzi (e il relativo utilizzo) delle password utilizzabili anche per l'accesso agli altri.

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

All'art. 30 il GDPR prevede che alcuni Titolari debbano tenere (e mettere a disposizione del Garante ove richiesto) un Registro delle attività di trattamento, una sorta di "**censimento dei trattamenti**", contenente varie informazioni sui trattamenti svolti, tra cui:

- i riferimenti del Titolare e del DPO se nominato
- le finalità del trattamento
- le categorie di interessati e dei dati personali trattati
- le categorie di destinatari a cui i dati vengono comunicati nonché l'eventuale paese straniero o organizzazione internazionale a cui i dati vengono trasferiti
- il momento della cancellazione dei dati
- se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

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

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

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

Le 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**:

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

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

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

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

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

Ecco le principali caratteristiche del Registro:

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

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

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

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

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

- vanno fornite **istruzioni scritte agli incaricati/autorizzati** per il controllo e la custodia degli atti e documenti contenenti dati personali

*Significa che l'associazione deve stabilire le modalità di **custodia, controllo e utilizzo dei documenti** contenenti dati personali (es. se c'è un archivio, chi lo custodisce, chi può accedervi e come, ecc.), dirette ad evitare l'accesso non consentito di terzi estranei. Tali modalità si possono anche solo risolvere nel non lasciare incustoditi presso la sede atti o documenti riguardanti l'ente o gli aderenti e nel riporli in appositi armadi chiusi a chiave, soprattutto se si tratta di dati sensibili.*

- vanno individuati gli **ambiti di trattamento** dei dati consentiti agli incaricati/autorizzati al trattamento o a categorie omogenee di incaricati e il loro aggiornamento almeno annuale
  Significa che l'associazione deve stabilire per iscritto le persone o le categorie omogenee (es. volontari, es. membri del consiglio, es. dipendenti) autorizzate a compiere le attività di trattamento dei dati, con specificazione dei limiti e modalità, e verificare ed eventualmente modificare tali incarichi almeno una volta l'anno. La verifica va fatta per i casi in cui l'incaricato cessi di trattare dati (es. recesso o esclusione dell'aderente, cessazione delle cariche o degli eventuali rapporti di lavoro ecc.) o venga modificato l'ambito del suo trattamento.
- va assicurato un **accesso controllato** agli archivi e documenti contenenti dati sensibili e/o giudiziari
  Significa che l'associazione deve far attenzione che i documenti/atti contenenti dati sensibili siano accessibili solo alle persone a ciò autorizzate e che costoro non lascino accedere terze persone nel corso del trattamento. L'accesso all'archivio (stanza dove stanno le banche dati cartacee) fuori dall'orario di apertura della sede deve essere registrato in un quaderno.

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

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

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

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

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

Si tratta di ipotesi che raramente interessano gli Enti del Terzo Settore, ad eccezione del trattamento di dati sensibili e giudiziari, per il quale è necessario capire quanto tale trattamento si svolge su larga scala. Come detto al **par. 14,** i trattamenti su LARGA SCALA sono stati identificati:

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

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

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

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

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

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

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

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

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

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

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

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

Consiglieri, volontari e dipendenti vanno tutti responsabilizzati sui rischi di data breach e devono tutti in grado di gestirli, nel senso di essere consapevoli su quello che debba essere fatto in caso di violazione e sugli obblighi di informazione.

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

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

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

Trattamento illecito di dati (art. 167)

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

La prima ipotesi di reato riguarda principalmente i "fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione pubblica accessibile al pubblico" (art. 123 e 126 Codice), la seconda riguarda tendenzialmente le Pubbliche Amministrazioni (art. 2 sexies Codice). Gli ambiti che potrebbero ipoteticamente riguardare un ente no

*profit sono la violazione dolosa delle regole stabilite dall'art. 130 del Codice sulle "**comunicazioni indesiderate**" automatiche, telefoniche, cartacee o elettroniche, per finalità di marketing, il trattamento di **dati sensibili o giudiziari** non conforme alla legge o in violazione delle misure di sicurezza stabilite dal Garante e il **trasferimento dei dati a paesi extra UE** che non abbiano adottato misure di sicurezza adegate. Tutti i reati presuppongono il **dolo specifico** di voler arricchire se stessi o altri o procurare un danno e l'esistenza di un pregiudizio (anche non economico) arrecato a terzi.*

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

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

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

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

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

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

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

*Ci si può chiedere a questo punto quale sia il **rischio concreto** per le associazioni 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 frequentemente dati sensibili, che sono quelli che vanno maggiormente tutelati.*

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

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

- art. 83 comma 4 GDPR: è soggetta alla **sanzione pecuniaria (multa) "fino a € 10.000.000,00**" la violazione dolosa o colposa degli obblighi gravanti sul Titolare e sul Responsabile del trattamento previsti dagli articoli 8, 11, da 25 a 39, 42 e 43; la violazione degli obblighi stabiliti dall'organismo di certificazione a norma degli articoli 42 e 43; la violazione degli obblighi stabiliti dall'organismo di controllo a norma dell'articolo 41, paragrafo 4.
  Si tratta ad esempio delle seguenti ipotesi: trattamento senza consenso dei dati del minore, mancata redazione dei Registri del trattamento o mancata adozione delle MISURE ADEGUATE, mancata notifica al Garante o all'interessato del DATA BREACH, mancata esecuzione della DSPIA, mancata designazione del DPO.
  Ulteriori ipotesi, per la maggior parte estranee ai trattamenti svolti dagli enti no profit, sono previste dall'art. 166 comma 1 del Codice aggiornato al GDPR

- art. 83 comma 5 GDPR: è soggetta alla **sanzione pecuniaria (multa) "fino a € 20.000.000,00**" ad esempio la violazione dolosa o colposa:
  a) dei "principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9";
  b) dei "diritti degli interessati a norma degli articoli da 12 a 22";
  c) delle regole per i "trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49";
  Si tratta di tutte le regole e i principi visti nei paragrafi di cui sopra sulla liceità, base giuridica e finalità dei trattamenti, sulla pertinenza ed esattezza dei dati, sul consenso al trattamento dei dati comuni e "particolari", sull'obbligo e contenuto dell'informativa e sugli altri diritti degli interessati (rettifica, oblio, limitazione, portabilità, opposizione).
  Ulteriori ipotesi sono previste dall'art. 166 comma 2 del Codice aggiornato al GDPR.

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

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

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

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

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

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

Le sanzioni amministrative vengono **decise dal Garante per la protezione dei dati personali**, anche su reclamo o segnalazione dell'interessato, dopo una fase istruttoria di accertamento (artt. 166 del Codice aggiornato al GDPR), nella quale il Garante può chiedere al titolare, al responsabile, all'interessato o a terzi di

fornire informazioni o esibire documenti. L'irrogazione della sanzione è disciplinata dalla L. n. 689/81 (sulle sanzioni amministrative, es. multe per eccesso di velocità): il Garante, se ritiene si sia compiuto l'illecito, notifica la contestazione; entro 60 giorni chi la riceve può far pervenire sue difese e chiedere di essere sentito; se il Garante conferma la violazione emette una ordinanza ingiunzione di pagamento, che è impugnabile davanti al giudice del luogo in cui è stato commesso l'illecito entro 30 giorni dalla notifica dell'ordinanza.

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

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

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

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

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

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

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

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

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

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

I principali consigli, quindi, che si possono fornire alle ODV, APS e in genere alle Associazioni ed enti no profit è quello di a) **non sottovalutare l'adeguamento al GDPR**, soprattutto se svolgono trattamenti di **dati particolarmente delicati** (dati ex sensibili, dati giudiziari, dati di minori, dati sanitari, ecc.) o trattamenti di dati di un numero rilevante di persone, specie se con modalità informatiche o "automatiche"; b) **evitare i gravi errori** e la loro ripetizione, che maggiormente possono generare danni ingenti; c) verificare che nelle **polizze assicurative di RC verso terzi** sia espressamente prevista (e comunque non esclusa) la responsabilità dell'associazione per danni causati a terzi dai propri amministratori e associati, per effetto di un'attività di trattamento posta in essere in violazione del GDPR e in generale della normativa europea e nazionale sul trattamento dei dati personali.

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

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

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

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

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

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

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

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

28. Cambia qualcosa se l'ente non profit ha rapporti con la pubblica amministrazione?

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

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

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

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

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

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

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

Piuttosto, soprattutto quando il trattamento dei dati è svolto dall'associazione esclusivamente nell'ambito della struttura pubblica e secondo le direttive della P.A., ma anche **quando l'attività di trattamento dei dati da parte dell'associazione è svolta "per conto" della Pubblica Amministrazione Titolare dei dati e per il perseguimento delle finalità proprie della P.A. o stabilite dalla P.A.** (es. dati di cittadini o di persone raccolti dalla P.A. e trasferiti all'ente no profit ai fini dell'esecuzione di un servizio di interesse generale assegnato all'ente no profit quale soggetto convenzionato o accreditato o quale appaltatore) **sussistono le condizioni per cui l'ente no profit sia nominato RESPONSABILE (ESTERNO) DEL TRATTAMENTO**, il che certamente comporta l'assunzione delle responsabilità collegate a tale ruolo (nella sostanza però comunque esistenti) ma permette all'Associazione di avere istruzioni scritte sulla durata, finalità e modalità del trattamento dei dati (vedi art. 28 comma 3 GDPR).

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

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

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

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

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

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

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

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

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

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

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

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

→ all'art. 130 comma 3 bis, che l'attività cd. di **spam "leggero"** e cioè quella svolta solo attraverso le chiamate telefoniche e la posta cartacea, è consentita anche senza previo consenso (cd. **opt-out**) a meno che la persona non abbia esercitato il **diritto di opposizione** nei cd. Registri pubblici delle opposizioni (in relazione agli elenchi telefonici il registro delle opposizioni è stato previsto e regolato in Italia con D.P.R. 178 del 7.9.2010 e risulta alla pagina web ***www.registrodelleopposizioni.it***; è prevista dalla recente L. n. 5/2018 anche l'istituzione di un Registro delle opposizioni riferito all'utilizzo dei numeri di cellulare e a tutti i numeri riservati non presenti negli elenchi telefonici pubblici).

Quindi certamente **le Associazioni possono contattare telefonicamente o spedire posta cartacea, per raccolta fondi o sensibilizzazione, alle persone che non sono presenti nel Registro delle opposizioni**

Va infine segnalato:

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

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

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

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

GUIDA OPERATIVA

A) ANALISI PRELIMINARE

1. **fare un "censimento" di tutti i trattamenti di dati personali svolti dall'Associazione**, verificandone la finalità, la tipologia di dati e di interessati, le modalità di raccolta, di conservazione e di utilizzo, i soggetti che svolgono i trattamenti, se i dati vengono comunicati a terzi e/o diffusi e che accorgimenti vengono posti in essere per evitare la perdita, la distruzione o l'accesso non autorizzato (→ **par. 2, 4, 10, 15, 16, 17 , 18, 19, 20, 21, 23, 28 e 29**)
2. **verificare se l'Associazione ha l'obbligo di redigere il Registro dei Trattamenti** (nel quale vanno inserite le informazioni del punto 1) **e in ogni caso valutare se**, per migliore organizzazione, **redigere il Registro a prescindere dall'esistenza dell'obbligo** (→ **par. 22**)
3. verificare se l'Associazione è autonomo **Titolare** del trattamento o se vi possono essere rapporti di **contitolarità** con eventuali livelli inferiori o superiori (→ **par. 5**)
4. stabilire quali sono all'interno dell'Associazione i **ruoli in ambito privacy**, ed in particolare se vi sono Responsabili (interni) del trattamento e quali sono le persone incaricate/autorizzate al trattamento, anche per categorie (→ **par. 15 e 20**)
5. verificare se è necessaria la nomina del **DPO - Data Protection Officer** (→ **par. 14**)
6. verificare se l'Associazione svolge uno o più trattamenti attraverso soggetti terzi che vanno nominati Responsabili (esterni) del trattamento (→ **par. 15**)
7. verificare se l'Associazione svolge per altri Titolari uno o più trattamenti tali per cui l'Associazione debba essere nominata Responsabile (esterno) del trattamento (→ **par. 15 e 28**)
8. verificare se uno o più trattamenti comportano il **trasferimento di dati al di fuori dell'Unione Europea** (→ **par. 27**)

B) PRINCIPI DEL TRATTAMENTO

1. trattare i dati in modo lecito e secondo correttezza, tutelando la riservatezza della persona, per le finalità statutarie (→ **par. 6**)
2. raccogliere, registrare ed utilizzare i dati solo per gli **scopi** determinati, espliciti e legittimi **indicati nello statuto** (→ **par. 6**)
3. fare in modo che i dati siano esatti, se necessario aggiornati, pertinenti, completi e non eccedenti rispetto agli scopi statutari e conservarli per un periodo di tempo non superiore a quello necessario per il raggiungimento di tali scopi (→ **par. 6 e 8**)

C) INFORMATIVA, CONSENSO E DIRITTI DEGLI INTERESSATI

1. **aggiornare le informative** da rivolgere agli interessati (soci/associati, i beneficiari e terzi, i dipendenti e collaboratori) rispetto alla situazione privacy attuale dell'Associazione, inserendovi l'ulteriore contenuto richiesto dall'art. 13 GDPR, e ritrasmetterle agli interessati o trasmetterle ex novo ai nuovi interessati che conferiscono i loro dati (→ **par. 7**)
2. chiedere il **consenso/autorizzazione al trattamento dei dati** quando necessario (→ **par. 10, 12 e 13**) previa comunicazione dell'informativa
3. assicurare a ogni interessato la possibilità di esercitare i **diritti di cui agli art. da 15 a 22 del GDPR**, eventualmente nominando un Incaricato con il compito di rispondere alla richiesta medesima (→ **par. 9**)
4. verificare il rispetto delle Autorizzazioni Generali del Garante (→ **par. 11**)

D) MISURE DI SICUREZZA

1. in caso di **TRATTAMENTO INFORMATICO DEI DATI**, adottare previamente misure di sicurezza adeguate ad evitare la perdita, la distruzione o l'accesso non autorizzato dei dati (→ **par. 17**) ed in particolare:

   → fornire alle persone che all'interno dell'Associazione trattano dati personali **istruzioni scritte/lettere di incarico** (nominative o per categorie di soggetti: es. volontari, soci, dirigenti, ecc.) sull'ambito del

trattamento consentito a ciascun incaricato/categoria e sulle modalità del trattamento (cd. *sistema di autorizzazione*) (→ **par. 17**)

- → attribuire a ciascun incaricato che utilizza il computer le **credenziali di autenticazione** (generalmente *username* e *password*) che gli consentano di accedere al computer e di svolgere i trattamenti a lui consentiti (cd. *sistema di autenticazione*) (→ **par. 18**)
- → dotare gli strumenti informatici dell'Associazione di idonei e aggiornati **sistemi di protezione** (antivirus, firewall, aggiornamento dei sistemi operativi e dei programmi, salvataggio dei dati in supporti esterni o in altri server, ecc.) (→ **par. 21**)
- → conservare adeguata documentazione, anche proveniente dalla ditta informatica, diretta a dimostrare l'avvenuta adozione delle suddette misure di sicurezza (→ **par. 17, 18, 19 e 21**)

2. in caso di **TRATTAMENTO CARTACEO DEI DATI**
   - → fornire alle persone che all'interno dell'Associazione trattano dati personali **istruzioni scritte/lettere di incarico** (nominative o per categorie di soggetti: es. volontari, soci, dirigenti, ecc.) sull'ambito del trattamento consentito a ciascun incaricato/categoria, sulle modalità di controllo e di custodia degli atti, dei documenti e dei fascicoli (→ **par. 23**)
3. in entrambi i casi, ove necessario, svolgere adeguata **FORMAZIONE** ai consiglieri, ai volontari e in genere agli incaricati del trattamento sugli obblighi derivanti dal GDPR, conservandone la relativa documentazione (es. registro presenze)

E) ULTERIORI IMPORTANTI ADEMPIMENTI

1. svolgere una **Valutazione di Impatto** sulla protezione dei dati (DPIA) nei casi previsti dall'art. 35 GDPR (→ **par. 24**)
2. in caso violazione di dati personali (**DATA BREACH**), svolgere le comunicazioni e attività previste dall'art. 33 e 34 GDPR (→ **par. 25**)

MODELLI DI DOCUMENTI

ATTENZIONE: i seguenti ESEMPI E MODELLI DI DOCUMENTI sono da utilizzare, integrare e modificare in relazione alla specifica realtà associativa e una volta esaminati i relativi argomenti nelle domande/risposte

INFORMATIVA EX ART. 13 GDPR PER SOCI E ASPIRANTI SOCI
E CONSENSO AL TRATTAMENTO

Caro socio/a o aspirante socio/a,
ai sensi degli art. 13 e 14 del Regolamento UE 2016/679 in materia di protezione dei dati personali ("GDPR") ti informiamo di quanto segue.
Finalità del trattamento e base giuridica. L'Associazione tratta i tuoi dati personali esclusivamente per lo svolgimento dell'attività istituzionale ed in particolare:

a) per la gestione del rapporto associativo (invio della corrispondenza, convocazione alle sedute degli organi, procedure amministrative interne) e per l'organizzazione ed esecuzione del servizio
b) per adempiere agli obblighi di legge (es. fiscali, assicurativi, ecc.) riferiti ai soci dell'Associazione;
c) per l'invio (tramite posta, posta elettronica, newsletter o numero di cellulare o altri mezzi informatici) di comunicazioni legate all'attività e iniziative dell'Associazione
d) in relazione alle immagini/video, per la pubblicazione nel sito dell'Associazione, sui social network dell'Associazione o su newsletter o su materiale cartaceo di promozione delle attività istituzionali dell'Associazione previo Tuo esplicito consenso
e) in relazione alla foto personale, per l'inserimento nel tesserino di riconoscimento
f) per la partecipazione dei soci a corsi, incontri e iniziative e per l'organizzazione e gestione dei corsi
g) per analisi statistiche, anche in forma aggregata.

La base giuridica del trattamento è rappresentata dalla richiesta di adesione e dal contratto associativo (art. 6 comma 1 lett. b GDPR), dal consenso al trattamento (art. 6 comma 1 lett. a – art. 9 comma 2 lett. a GDPR), dai contatti regolari con l'Associazione (art. 9 comma 2 lett. d GDPR), dagli obblighi legali a cui è tenuta l'Associazione (art. 6 comma 1 lett. c GDPR)
Modalità e principi del trattamento. Il trattamento avverrà nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, con modalità cartacee ed informatiche, ad opera di persone autorizzate dall'Associazione e con l'adozione di misure adeguate di protezione, in modo da garantire la sicurezza e la riservatezza dei dati. *Non verrà svolto alcun processo decisionale automatizzato.*
Necessità del conferimento. Il conferimento dei dati anagrafici e di contatto è necessario in quanto strettamente legato alla gestione del rapporto associativo. *Il consenso all'utilizzo delle immagini/video e alla diffusione dei dati nel sito istituzionale e nelle altre modalità sopra descritte è facoltativo.*
Comunicazione dei dati e trasferimento all'estero dei dati. *I dati potranno essere comunicati agli altri soci ai fini ai fini dell'organizzazione ed esecuzione del servizio.* I dati potranno essere comunicati ai soggetti deputati allo svolgimento di attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, assicuratore, sistemista, ecc.) e a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale allo svolgimento dell'attività istituzionale (formatori, Enti Locali, ditte che curano la manutenzione informatica, società organizzatrici dei corsi, ecc.). I dati potranno essere trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali, o comunque previa verifica che il destinatario garantisca adeguate misure di protezione. Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per lo svolgimento di attività per conto dell'Associazione saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR.
Periodo di conservazione dei dati. I dati saranno utilizzati dall'Associazione fino alla cessazione del rapporto associativo. Dopo tale data, saranno conservati per finalità di archivio, obblighi legali o contabili o fiscali o per esigenze di tutela dell'Associazione, con esclusione di comunicazioni a terzi e diffusione in ogni caso applicando i principi di proporzionalità e minimizzazione.
Diritti dell'interessato. Nella qualità di interessato, Ti sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora tu ritenga che il trattamento che ti riguarda violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede dell'Associazione.
*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*
Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Io sottoscritto/a, _____, nella qualità di interessato, letta la suddetta informativa resa ai sensi dell'art. 13 GDPR, **autorizzo/do il consenso**

□ al trattamento dei miei dati personali, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 **(*)**

□ *alla diffusione del mio nome e cognome, della mia immagine o di video che mi riprendono nel sito istituzionale, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo dell'Associazione, per soli fini di descrizione e promozione dell'attività istituzionale, nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 e delle autorizzazioni/indicazioni della Commissione UE e del Garante per la Protezione dei Dati Personali* **(**)**

_____, lì _____

L'INTERESSATO
(firma leggibile)

_____

(*) Il consenso al trattamento è indispensabile ai fini del perseguimento delle finalità associative e quindi la mancata autorizzazione comporta l'impossibilità di perfezionare l'adesione o il mantenimento della qualifica di socio
(**) Il consenso al trattamento è facoltativo

INFORMATIVA EX ART. 13 GDPR PER SOCI E ASPIRANTI SOCI MINORENNI E CONSENSO AL TRATTAMENTO

Gentile Signore/a,
ai sensi degli art. 13 e 14 del Regolamento UE 2016/679 in materia di protezione dei dati personali ("GDPR") La informiamo di quanto segue.
Finalità del trattamento e base giuridica. L'Associazione tratterà i dati personali di Suo figlio/a esclusivamente per lo svolgimento dell'attività istituzionale ed in particolare:

a) per la gestione del rapporto associativo (invio della corrispondenza, convocazione alle sedute degli organi, procedure amministrative interne
b) per adempiere agli obblighi di legge (es. fiscali, assicurativi, ecc.) riferiti ai soci dell'Associazione;
c) per l'invio (tramite posta, indirizzo e-mail o numero di cellulare o altri mezzi informatici) di comunicazioni legate all'attività e iniziative dell'Associazione
d) in relazione alle immagini o video di Suo figlio/a, per la pubblicazione sul sito dell'Associazione, sulla pagina FB dell'Associazione o su newsletter o su materiale di promozione delle attività istituzionali dell'Associazione previo Suo esplicito consenso
e) in relazione alla foto personale, per l'inserimento nel tesserino di riconoscimento
f) per la partecipazione dei soci a corsi, incontri e iniziative e per l'organizzazione e gestione dei corsi
g) per analisi statistiche, anche in forma aggregata.

La base giuridica del trattamento è rappresentata dalla richiesta di adesione e dal contratto associativo (art. 6 comma 1 lett. b GDPR), dal consenso al trattamento (art. 6 comma 1 lett. a – art. 9 comma 2 lett. a GDPR), dai contatti regolari con l'Associazione (art. 9 comma 2 lett. d GDPR), dagli obblighi legali a cui è tenuta l'Associazione (art. 6 comma 1 lett. c GDPR)
Modalità e principi del trattamento. Il trattamento avverrà nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, con modalità cartacee ed informatiche, ad opera di persone autorizzate dall'Associazione e con l'adozione di misure adeguate di protezione, in modo da garantire la sicurezza e la riservatezza dei dati. *Non verrà svolto alcun processo decisionale automatizzato.*
Necessità del conferimento. Il conferimento dei dati anagrafici e di contatto è necessario in quanto strettamente legato alla gestione del rapporto associativo. *Il consenso all'utilizzo delle immagini/video e alla diffusione dei dati nel sito istituzionale e nelle altre modalità sopra descritte è facoltativo.*
Comunicazione e trasferimento all'estero dei dati. I dati potranno essere comunicati ai soggetti deputati allo svolgimento di attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, assicuratore, sistemista, ecc.) e a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale allo svolgimento dell'attività istituzionale (formatori, Enti Locali, ditte che curano la manutenzione informatica, società organizzatrici dei corsi, ecc.). I dati potranno essere trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali, o comunque previa verifica che il destinatario garantisca adeguate misure di protezione. Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per lo svolgimento di attività per conto dell'Associazione saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR.
Periodo di conservazione dei dati. I dati saranno utilizzati dall'Associazione fino alla cessazione del rapporto associativo. Dopo tale data, saranno conservati per finalità di archivio, obblighi legali o contabili o fiscali o per esigenze di tutela dell'Associazione, con esclusione di comunicazioni a terzi e in ogni caso applicando i principi di proporzionalità e minimizzazione.
Diritti dell'interessato. Nella qualità di interessato, sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora Lei ritenga che il trattamento che riguarda Suo figlio/a violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede dell'Associazione.
*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*
Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Io sottoscritto/a _____, nella qualità di genitore di mio figlio/a _____, in conformità alle norme sulla responsabilità genitoriale di cui agli artt. 316, 337 ter e 337 quater del codice civile, letta la suddetta informativa resa ai sensi dell'art. 13 GDPR, **autorizzo/do il consenso**

☐ al trattamento dei **dati personali**, comuni e "particolari", di mio figlio/a, da svolgersi in conformità a quanto indicato nella suddetta informativa. **(*)**

☐ *alla diffusione del nome e cognome di mio figlio, della sua immagine o di video che lo riprendono, nel sito istituzionale, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo dell'Associazione, per soli fini di descrizione e promozione dell'attività istituzionale, nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 e delle autorizzazioni/indicazioni della Commissione UE e del Garante per la Protezione dei Dati Personali **(**)***

_____, lì _____

Il padre
(firma leggibile)

_____

la madre
(firma leggibile)

_____

(*) Il consenso al trattamento è indispensabile ai fini del perseguimento delle finalità associative e quindi la mancata autorizzazione comporta l'impossibilità di perfezionare l'adesione o il mantenimento della qualifica di socio
(**) Il consenso al trattamento è facoltativo

INFORMATIVA EX ART. 13 GDPR PER BENEFICIARI ED ESTERNI E CONSENSO AL TRATTAMENTO

Gentile Signore/a,
ai sensi degli art. 13 e 14 del Regolamento UE 2016/679 in materia di protezione dei dati personali ("GDPR") La informiamo di quanto segue.
Finalità del trattamento e base giuridica. L'Associazione tratterà i dati personali che La riguardano o da Lei conferiti esclusivamente per l'esecuzione della Sua richiesta o del servizio da Lei richiesto, la gestione dell'eventuale contratto/convenzione o altro rapporto e per l'adempimento dei relativi obblighi di legge. La base giuridica del trattamento è rappresentata dal contratto (art. 6 comma 1 lett. b GDPR) o da un obbligo legale (art. 6 comma 1 lett. c GDPR).
Modalità e principi del trattamento. Il trattamento avverrà nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, con modalità cartacee ed informatiche, ad opera di persone autorizzate dall'Associazione e con l'adozione di misure adeguate di protezione, in modo da garantire la sicurezza e la riservatezza dei dati. *Non verrà svolto alcun processo decisionale automatizzato.*
Necessità del conferimento. Il conferimento dei dati è necessario in quanto strettamente legato all'organizzazione del servizio e alla gestione del contratto o rapporto. *Ove il servizio consista nella partecipazione ad eventi, corsi o attività dell'Associazione, potranno essere acquisite e pubblicate nel sito istituzionale, nei social network e sul materiale informativo cartaceo dell'Associazione Sue immagini fotografiche o video, solo previo esplicito e separato consenso da Lei espresso.*
Comunicazione e trasferimento all'estero dei dati. I dati potranno essere comunicati ai soggetti deputati allo svolgimento dei servizi e attività richieste (es. formatori esterni) e alle attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, assicuratore, sistemista, ecc.). *I dati potranno essere trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali, o comunque previa verifica che il destinatario garantisca adeguate misure di protezione*. Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per lo svolgimento di attività per conto dell'Associazione saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR.
Periodo di conservazione dei dati. Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti (svolgimento del servizio o esecuzione della richiesta), fatti salvi gli obblighi legali o contabili o fiscali o la sussistenza di esigenze di tutela legale dell'Associazione, con esclusione di comunicazioni a terzi e in ogni caso applicando i principi di proporzionalità e minimizzazione.
Diritti dell'interessato. Nella qualità di interessato, Le sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora tu ritenga che il trattamento che ti riguarda violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede dell'Associazione.
*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*
Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Io sottoscritto/a, _____, nella qualità di interessato, letta la suddetta informativa resa ai sensi dell'art. 13 GDPR, **autorizzo/do il consenso**

- □ al trattamento dei miei dati personali, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 **(*)**
- □ *all'utilizzo del mio indirizzo e-mail al fine dell'invio della newsletter periodica dell'Associazione* **(**)**
- □ *alla diffusione della mia immagine o di video che mi riprendono nel sito istituzionale, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo dell'Associazione, per soli fini di descrizione e promozione dell'attività istituzionale, nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 e delle autorizzazioni/indicazioni della Commissione UE e del Garante per la Protezione dei Dati Personali* **(**)**

_____, lì _____

L'INTERESSATO
(firma leggibile)

_____

(*) Il consenso al trattamento è indispensabile ai fini dell'esecuzione del servizio richiesto
(**) Il consenso al trattamento è facoltativo

INFORMATIVA EX ART. 13 GDPR PER BENEFICIARI ED ESTERNI MINORENNI E CONSENSO AL TRATTAMENTO

Gentile Signore/a,
ai sensi degli art. 13 e 14 del Regolamento UE 2016/679 in materia di protezione dei dati personali ("GDPR") La informiamo di quanto segue.
Finalità del trattamento e base giuridica. L'Associazione tratterà i dati personali di Suo figlio/a da Lei conferiti esclusivamente per l'esecuzione della Sua richiesta o del servizio da Lei richiesto e per l'adempimento dei relativi obblighi di legge. La base giuridica del trattamento è rappresentata dal contratto (art. 6 comma 1 lett. b GDPR) o da un obbligo legale (art. 6 comma 1 lett. c GDPR).
Modalità e principi del trattamento. Il trattamento avverrà nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, con modalità cartacee ed informatiche, ad opera di persone autorizzate dall'Associazione e con l'adozione di misure adeguate di protezione, in modo da garantire la sicurezza e la riservatezza dei dati. *Non verrà svolto alcun processo decisionale automatizzato.*
Necessità del conferimento. Il conferimento dei dati è necessario in quanto strettamente legato all'organizzazione del servizio richiesto. *Ove il servizio consista nella partecipazione ad eventi, corsi o attività dell'Associazione, potranno essere acquisite e pubblicate nel sito istituzionale, nei social network e sul materiale informativo cartaceo dell'Associazione immagini fotografiche o video di Suo figlio/a, solo previo esplicito e separato consenso da Lei espresso.*
Comunicazione e trasferimento all'estero dei dati. I dati potranno essere comunicati ai soggetti deputati allo svolgimento dei servizi e attività richieste (es. formatori esterni) e alle attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, assicuratore, sistemista, ecc.). *I dati potranno essere trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali, o comunque previa verifica che il destinatario garantisca adeguate misure di protezione*. Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per lo svolgimento di attività per conto dell'Associazione saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR.
Periodo di conservazione dei dati. Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti (svolgimento del servizio o esecuzione della richiesta), fatti salvi gli obblighi legali o contabili o fiscali o la sussistenza di esigenze di tutela legale dell'Associazione, con esclusione di comunicazioni a terzi e in ogni caso applicando i principi di proporzionalità e minimizzazione.
Diritti dell'interessato. Nella qualità di interessato, sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora tu ritenga che il trattamento che ti riguarda violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede dell'Associazione.
*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*
Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Io sottoscritto/a _____, nella qualità di genitore di mio figlio/a _____, in conformità alle norme sulla responsabilità genitoriale di cui agli artt. 316, 337 ter e 337 quater del codice civile, letta la suddetta informativa resa ai sensi dell'art. 13 GDPR, **autorizzo/do il consenso**

□ al trattamento dei dati personali di mio figlio/a, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 **(*)**

□ *all'utilizzo del mio indirizzo e-mail o di quello di mio figlio al fine dell'invio della newsletter periodica dell'Associazione* **(**)**

□ *alla diffusione dell'immagine o di video che riprendono mio figlio/a nel sito istituzionale, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo dell'Associazione, per soli fini di descrizione e promozione dell'attività istituzionale, nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 e delle autorizzazioni/indicazioni della Commissione UE e del Garante per la Protezione dei Dati Personali* **(**)**

_____, lì _____

Il padre
(firma leggibile)

_____

la madre
(firma leggibile)

_____

(*) Il consenso al trattamento è indispensabile ai fini dell'esecuzione del servizio richiesto
(**) Il consenso al trattamento è facoltativo

INFORMATIVA EX ART. 13 GDPR PER CONSULENTI COLLABORATORI E FORNITORI E CONSENSO AL TRATTAMENTO

Egregio Signore/a,
ai sensi dell'art. 13 del Regolamento UE 2016/679 in materia di protezione dei dati personali ("GDPR") La informiamo di quanto segue.
Finalità del trattamento e base giuridica. L'Associazione tratterà i dati personali che La riguardano o da Lei conferiti esclusivamente nell'ambito del rapporto di consulenza, collaborazione o fornitura (ai fini dell'adempimento degli obblighi contrattuali e di legge, per la corrispondenza e per la rintracciabilità, per l'organizzazione del servizio, ecc.). La base giuridica è rappresentata dal contratto (art. 6, comma 1, lett. b e art. 9 comma 2 lett. b GDPR), dagli obblighi legali a cui è tenuta l'Associazione (art. 6 comma 1 lett. c GDPR) e dal consenso (art. 6 comma 1 lett. a e art. 9 comma 2 lett. a GDPR).
Dati sensibili. Il trattamento di Suoi eventuali dati "particolari" e relativi alla salute sarà effettuato nei limiti di cui all'art. 9 comma 2 lett. b) e lett. h GDPR e quindi solo ove il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti in materia di diritto del lavoro, sicurezza sociale e protezione sociale.
Modalità e principi del trattamento. Il trattamento avverrà nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, con modalità cartacee ed informatiche, ad opera di persone autorizzate dall'Associazione e con l'adozione di misure adeguate di protezione, in modo da garantire la sicurezza e la riservatezza dei dati. *Non verrà svolto alcun processo decisionale automatizzato.*
Necessità del conferimento. Comunicazione e trasferimento all'estero dei dati. Il conferimento dei dati è necessario in quanto strettamente legato all'organizzazione del servizio e alla gestione del rapporto. I dati potranno essere comunicati a tutti i soggetti deputati allo svolgimento di attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, consulente del lavoro, assicuratore, sistemista, ecc.) e a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale allo svolgimento dell'attività istituzionale e alla gestione del rapporto di lavoro (I.N.P.S., I.N.A.I.L., formatori, Enti Locali, Enti sanitari, fornitori, ecc.). Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per lo svolgimento di attività per conto dell'Associazione saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR. I dati potranno essere trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali, o comunque previa verifica che il destinatario garantisca adeguate misure di protezione.
Periodo di conservazione dei dati. I dati saranno utilizzati dall'Associazione per tutta la durata del rapporto. Dopo tale data, saranno conservati i soli dati la cui conservazione risponde ad obblighi legali o contabili o fiscali o ad esigenze di tutela dell'Associazione.
Diritti dell'interessato. Nella qualità di interessato, Le sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora tu ritenga che il trattamento che ti riguarda violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede dell'Associazione.
*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*
Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Io sottoscritto/a, _____, nella qualità di interessato, letta la suddetta informativa resa ai sensi dell'art. 13 GDPR, **autorizzo/do il consenso**

□ al trattamento dei miei dati personali, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 **(*)**

□ *alla diffusione del mio nome e cognome, ruolo e immagine fotografica sul sito istituzionale dell'Associazione* **(**)**

_____, lì _____

L'INTERESSATO
(firma leggibile)

_____

(*) Il consenso al trattamento è indispensabile ai fini della gestione del rapporto di lavoro
(**) Il consenso al trattamento è facoltativo

INFORMATIVA EX ART. 13 GDPR PER DIPENDENTI
E CONSENSO AL TRATTAMENTO

Egregio Signore/a,
ai sensi dell'art. 13 del Regolamento UE 2016/679 in materia di protezione dei dati personali ("GDPR") La informiamo di quanto segue.
Finalità del trattamento e base giuridica. L'Associazione tratterà i dati personali che La riguardano o da Lei conferiti esclusivamente nell'ambito del rapporto di lavoro o della collaborazione professionale (ai fini dell'adempimento degli obblighi contrattuali e di legge, per la corrispondenza e per la rintracciabilità, per l'organizzazione del servizio, ecc.). La base giuridica è rappresentata dal contratto di lavoro (art. 6, comma 1, lett. b e art. 9 comma 2 lett. b GDPR), dagli obblighi legali a cui è tenuta l'Associazione (art. 6 comma 1 lett. c GDPR) e dal consenso (art. 6 comma 1 lett. a e art. 9 comma 2 lett. a GDPR).
Dati sensibili. Il trattamento di Suoi eventuali dati "particolari" e relativi alla salute sarà effettuato nei limiti di cui all'art. 9 comma 2 lett. b) e lett. h GDPR e quindi solo ove il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti in materia di diritto del lavoro, sicurezza sociale e protezione sociale.
Modalità e principi del trattamento. Il trattamento avverrà nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, con modalità cartacee ed informatiche, ad opera di persone autorizzate dall'Associazione e con l'adozione di misure adeguate di protezione, in modo da garantire la sicurezza e la riservatezza dei dati. *Non verrà svolto alcun processo decisionale automatizzato.*
Necessità del conferimento. Comunicazione e trasferimento all'estero dei dati. Il conferimento dei dati è necessario in quanto strettamente legato all'organizzazione del servizio e alla gestione del rapporto di lavoro. *La pubblicazione del cognome e nome, del ruolo e dell'indirizzo e-mail sul sito dell'Associazione, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo dell'Associazione è invece facoltativa e avviene solo previo esplicito e specifico consenso*. I dati potranno essere comunicati a tutti i soggetti deputati allo svolgimento di attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, consulente del lavoro, assicuratore, sistemista, ecc.) e a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale allo svolgimento dell'attività istituzionale e alla gestione del rapporto di lavoro (I.N.P.S., I.N.A.I.L., formatori, Enti Locali, Enti sanitari, fornitori, ecc.). Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per lo svolgimento di attività per conto dell'Associazione saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR. I dati potranno essere trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali, o comunque previa verifica che il destinatario garantisca adeguate misure di protezione.
Periodo di conservazione dei dati. I dati saranno utilizzati dall'Associazione per tutta la durata del rapporto lavorativo. Dopo tale data, saranno conservati i soli dati la cui conservazione risponde ad obblighi legali o contabili o fiscali o ad esigenze di tutela dell'Associazione.
Diritti dell'interessato. Nella qualità di interessato, Le sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora tu ritenga che il trattamento che ti riguarda violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede dell'Associazione.
*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*
Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Io sottoscritto/a, _____, nella qualità di interessato, letta la suddetta informativa resa ai sensi dell'art. 13 GDPR, **autorizzo/do il consenso**

- ☐ al trattamento dei miei dati personali, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 **(*)**
- ☐ *alla diffusione del mio nome e cognome, ruolo e immagine fotografica sul sito istituzionale dell'Associazione* **(**)**
- ☐ *alla diffusione della mia immagine o di video che mi riprendono nel sito istituzionale, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo dell'Associazione, per soli fini di descrizione e promozione dell'attività istituzionale, nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 e delle autorizzazioni/indicazioni della Commissione UE e del Garante per la Protezione dei Dati Personali* **(**)**

_____, lì _____

L'INTERESSATO
(firma leggibile)

_____

(*) Il consenso al trattamento è indispensabile ai fini della gestione del rapporto di lavoro
(**) Il consenso al trattamento è facoltativo

INFORMATIVA EX ART. 13 GDPR PER UTENTI DEL SITO

Ai sensi dell'art. 13 del Regolamento UE n. 2016/679 ("General Data Protection Regulation" o "GDPR") L'Associazione _____ rende noto a coloro ("utenti" o "interessati") che accedono al sito istituzionale a partire dall'indirizzo _____e che utilizzano i servizi disponibili in via telematica sul sito istituzionale, le seguenti informazioni. La presente informativa è resa esclusivamente in relazione al sito dell'Associazione e non anche in relazione ad altri siti web che possono essere consultati dall'utente tramite link riportati o accessibili nel portale medesimo.

Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

Finalità del trattamento e base giuridica. I dati personali acquisiti mediante il sito saranno trattati dall'Associazione, senza il consenso dell'interessato, ai sensi dell'art. 6 lett. b) ed e) del GDPR, per gestire e mantenere il sito, per consentire la fruizione dei servizi e il soddisfacimento delle richieste degli utenti, per consentire un'efficace comunicazione istituzionale, per adempiere agli obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria o da un ordine dell'Autorità o comunque connessi alle attività e funzioni istituzionali, o infine per prevenire o scoprire attività fraudolente o abusi a danno dell'Associazione attraverso il sito.

L'invio di posta elettronica agli indirizzi istituzionali indicati nel portale e la compilazione di format comportano la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella mail o nel format. In tal caso i dati acquisiti saranno trattati esclusivamente per rispondere alle richieste degli utenti. Specifiche informative o indicazioni sulla normativa/base giuridica di riferimento potranno essere inserite, in relazione ai particolari trattamenti di dati, in specifiche pagine del sito, nei format o nei modelli di documenti pubblicati nel sito.

Luogo e modalità del trattamento. Il trattamento dei dati acquisiti mediante il sito e/o connessi ai servizi del sito si svolge presso gli Uffici dell'Associazione ed eventualmente presso altri soggetti o sistemi informatici/server di altri soggetti appositamente designati come Responsabili (esterni) del trattamento. Il trattamento dei dati avviene sia in via cartacea sia mediante l'utilizzo di strumenti informatici, secondo i principi di correttezza, liceità, trasparenza, pertinenza e non eccedenza rispetto alle finalità di raccolta e di successivo trattamento e previa adozione le misure di sicurezza adeguate volte a prevenire la perdita dei dati, gli usi illeciti o non corretti, gli accessi non autorizzati ed in generale volte ad assicurare il rispetto delle previsioni del GDPR e del D. Lgs. n. 193/2006 e ss.mm. I dati sono trattati esclusivamente da personale, amministrativo e tecnico, autorizzato al trattamento o da eventuali persone autorizzate per occasionali operazioni di manutenzione. Il sito e i servizi on line non sono destinati a minori di 18 anni. I dati relativi a minori potranno essere trasmessi all'Associazione tramite l'accesso al sito e ai servizi solamente dai soggetti esercitanti la responsabilità genitoriale.

Obbligo o facoltà di conferire i dati. L'utente è libero di fornire i dati personali inseriti nei format di richiesta. Il mancato conferimento dei dati necessari a rendere il servizio può comportare l'impossibilità di ottenere quanto richiesto.

Periodo di conservazione. Ai sensi dell'art. 5 GDPR, i dati verranno trattati e conservati per un periodo di tempo non superiore al conseguimento delle finalità proprie del servizio e del trattamento e/o nel rispetto dei termini previsti da norme di legge o regolamento.

Comunicazione e diffusione dei dati. I dati conferiti dagli Utenti non sono destinati a terzi e non saranno oggetto di comunicazione o diffusione, salvo che disposizioni di legge o di regolamento dispongano diversamente (in particolare i dati potranno essere comunicati a Organismi di vigilanza, Autorità giudiziarie nonché a tutti gli altri soggetti ai quali la comunicazione sia obbligatoria per legge per l'espletamento delle suddette finalità.

Trasferimento dei dati all'estero. I dati non vengono trasferiti a paesi terzi al di fuori dello Spazio Economico Europeo.

Diritti dell'interessato. All'utente/interessato sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora si ritenga che il trattamento violi il Regolamento. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo posta elettronica, p.e.c. o fax, o a mezzo Raccomandata presso la sede dell'Associazione.

*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*

Accesso a siti esterni collegati. Il portale contiene collegamenti con siti di terze parti per ulteriore convenienza ed informazione dell'utente. Quando l'utente utilizza questi collegamenti abbandona il sito istituzionale dell'Associazione accedendo ad un sito diverso, sul quale l'Associazione non ha il controllo e in ordine al quale non ha responsabilità di sorta in materia di trattamento dei dati. Si consiglia pertanto di esaminare la policy di ogni sito che viene visitato.

Utilizzo dei cookies

I cookies sono file di testo che ciascun sito web invia a chi accede al sito stesso e che vengono ritrasmessi dal computer dell'utente al sito medesimo alla visita successiva.

***Cookies tecnici**. Il sito dell'Associazione utilizza cookie tecnici per consentire l'esplorazione sicura, rapida ed efficiente del sito stesso e per fornire agli utenti i servizi richiesti. Per l'installazione di tali cookie non è richiesto il preventivo consenso degli utenti.*

***Cookies tecnici di sessione**. Il sito dell'Associazione utilizza cookies di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser), limitatamente alla trasmissione di identificativi di sessione necessari per consentire l'esplorazione sicura ed efficiente da parte dell'utente. I cookies di sessione utilizzati evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificati dell'utente, e quindi non richiedono l'acquisizione del consenso dell'utente.*

***Cookies analitici**. Come avviene nella maggior parte dei siti web, il portale raccoglie informazioni relative alla navigazione degli utenti (es. collocazione geografica del fornitore di accesso a internet, tipo di browser utilizzato, indirizzo IP, pagine visitate sul sito, numero di utenti, ecc.), esclusivamente per finalità statistiche, senza che sia possibile l'identificazione individuale dell'utente. I dati ricavabili da questi cookie sono gestiti dall'Associazione in qualità di gestore del sito esclusivamente per finalità statistiche, per l'elaborazione di report sull'utilizzo del sito, per il miglioramento del contenuto del sito e per renderne più semplice l'uso.*

***Cookies di profilazione**. Il sito non utilizza cookie di profilazione, cioè cookies volti a creare profili relativi all'utente al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate nell'ambito della navigazione sul sito, o per la trasmissione di informazioni di carattere personale, né vengono utilizzati i c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.*

***Cookies di terzi**. Le società che inviano contenuti al portale dell'Associazione e quelle raggiungibili mediante links dalle pagine del portale (es. You tube, Facebook, ecc.) possono, a loro scelta, utilizzare "cookies" anche persistenti sui computer degli utenti, finalizzati alla memorizzazione dei dati di navigazione dell'utente, a partire dal momento nel quale l'utente clicca sul relativo link. In questo caso, l'utilizzo dei "cookies" esula dal controllo dell'Associazione. La maggior parte dei browsers accettano automaticamente i cookies, ma è possibile anche rifiutarli completamente, o accettarne selettivamente solo alcuni, modificando le impostazioni di sicurezza del browser (Internet Explorer, Google Chrome, Mozilla Firefox, Safari Opera, ecc.). Ciascun browser presenta procedure diverse per la gestione delle impostazioni. Se l'utente inibisce il caricamento dei cookies, alcune componenti del sito potrebbero essere non disponibili e certe pagine potrebbero risultare incomplete.*

INFORMATIVA EX ART. 13 GDPR PER ISCRITTI ALLA NEWSLETTER

Gentile interessato/a,
ricevi questa e-mail perché chiedi di essere iscritto o sei iscritto alla newsletter dell'Associazione _____ in virtù della domanda effettuata sul nostro portale o con altre modalità. Con la presente siamo a informarti sulle modalità del trattamento dei tuoi dati ai sensi dell'art. 13 del Regolamento UE/2016/679 ("GDPR").

Titolare del trattamento. Il titolare del trattamento è l'Associazione _____, con sede in _____ – tel. _____ – fax _____ – mail _____

Finalità e modalità di trattamento. Il trattamento dei dati verrà svolto, nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, esclusivamente per l'invio della newsletter periodica sulle iniziative e attività dell'Associazione, ivi incluse eventuali campagne di sensibilizzazione e raccolta fondi e eventuali newsletter straordinarie per informazioni di carattere generale o urgente. Il Trattamento avverrà con modalità informatiche, ad opera di persone autorizzate dall'Associazione e con l'adozione di misure adeguate di protezione, in modo da garantire la sicurezza e la riservatezza dei dati. *Non verrà svolto alcun processo decisionale automatizzato.* La base giuridica del trattamento è rappresentata dalla richiesta di iscrizione al servizio di newsletter (art. 6 comma 1 lett. b GDPR).

Comunicazione e trasferimento all'estero dei dati. *I dati saranno conservati presso i server host e SMTP che garantisce di adottare parametri di sicurezza e protezione dei dati adeguati al GDPR* [*oppure*] *Ai soli fini del servizio di newsletter, i dati sono trasmessi a destinatari con sede extra UE (es. Google LLC o Mailchimp/Rocket Science Group LCC) i cui Stati hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati.* Al di fuori del trattamento sopra descritto, i dati non sono comunicati a terzi (né a Paesi terzi) né sono diffusi. Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per la gestione informatica del servizio di newsletter saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR.

Necessità del conferimento. Il conferimento e l'uso dell'indirizzo e-mail sono necessari per ricevere la newsletter. Il conferimento degli altri dati è facoltativo.

Periodo di conservazione dei dati. I dati personali saranno conservati ed utilizzati per il tempo necessario all'invio della newsletter periodica, e verranno cancellati in caso di revoca dell'iscrizione alla newsletter medesima.

Diritti dell'interessato. Nella qualità di interessato, Ti sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR, tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora tu ritenga che il trattamento che ti riguarda violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede dell'Associazione.

*Il **Data Protection Officer** (DPO) nominato dall'Associazione è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dall'Associazione e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.*

GESTIONE DEI TUOI DATI PERSONALI: puoi gestire i tuoi dati e l'adesione alla newsletter, in qualsiasi momento, dai link in calce ad ogni comunicazione inviata per mezzo della newsletter.

ATTO DI NOMINA A RESPONSABILE / REFERENTE (INTERNO)
DEL TRATTAMENTO DEI DATI

L'associazione _____ (C.F. _____; tel. _____; fax _____; mail _____), con sede in _____, Titolare del trattamento ai sensi dell'art. 4 comma 1 n. 7 GDPR, in persona del Presidente e legale rappresentante _____

NOMINA

RESPONSABILE / DELEGATO (INTERNO) DEL TRATTAMENTO DEI DATI

Il/La Signor/a _____ (C.F. _____), nato/a a _____in data _____, tel. _____, mail _____, che all'interno dell'Associazione ha la qualifica di _____, di seguito indicato anche quale "Responsabile interno", secondo i criteri, le modalità e le istruzioni di seguito specificate.

Il Responsabile interno ha il compito di compiere tutto quanto si renderà necessario ai fini di assicurare il rispetto e la corretta applicazione, da parte dell'Associazione, degli obblighi, disposizioni e principi di cui al GDPR e del D.Lgs. n. 196 del 30.6.2003 (Codice in materia di trattamento dei dati personali) ove applicabili.

In particolare e ai tali fini, spetta al Responsabile interno:

- nominare o far nominare per iscritto dal Titolare gli Incaricati del trattamento, fornendo loro istruzioni operative e vigilando sul rispetto di dette istruzioni;
- individuare i Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR e proporre al Titolare la stipula del relativo Accordo/contratto;
- classificare le banche dati e proporre al Titolare un sistema complessivo di trattamento dei dati personali, comuni e "particolari", dell'Associazione;
- ai sensi dell'art. 25 GDPR, e in relazione alla natura, ambito di applicazione, contesto e finalità dei trattamenti, nonché in considerazione dei rischi per i diritti e le libertà delle persone fisiche, proporre al Titolare, anche in collaborazione con un esperto informatico, l'adozione di misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, nonché al fine di garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento; se del caso proporre al Titolare l'adesione ai codici di condotta di cui all'art. 40 GDPR o a un meccanismo di certificazione di cui all'art. 42 GDPR;
- collaborare con la ditta incaricata della manutenzione e aggiornamento delle banche dati informatiche e del sistema informatico al fine di assicurare, ai sensi dell'art. 32 GDPR, l'adozione e la conservazione di misure e procedure informatiche adeguate e vigilare sul rispetto di dette misure da parte degli Incaricati, al fine di impedire trattamenti non autorizzati o illeciti o la perdita, la distruzione o il danno accidentale delle banche dati o dei dati personali (principio di integrità e riservatezza);
- attuare e far eseguire gli obblighi di informativa ex art. 13 e 14 GDPR e di acquisizione del consenso degli interessati ex art. 7, 8, 9 e 10 GDPR;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dagli artt. 15, 16, 17, 18, 20, 21 GDPR;
- assicurare, in caso di violazione dei dati personali, l'esecuzione degli obblighi di notifica di cui all'art. 33 GDPR e di comunicazione di cui all'art. 34 GDPR;
- svolgere ogni iniziativa e attività più opportuna per l'attuazione di eventuali prescrizioni del DPO ove nominato o del Garante per la Protezione dei dati Personali;
- redigere e tenere aggiornato il Registro dei Trattamenti di cui all'art. 30 GDPR, ove obbligatorio o comunque ove adottato;
- valutare unitamente al DPO, ove nominato, l'opportunità di svolgere una valutazione di impatto ai sensi dell'art. 35 GDPR e/o una consultazione preventiva ai sensi dell'art. 36 GDPR e, in caso positivo, collaborare con il Titolare e altri eventuali Referenti nello svolgimento di dette operazioni;
- assicurare che qualunque trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale avvenga nel rispetto dei principi e prescrizioni di cui agli artt. 44ss GDPR;
- dare immediata comunicazione al Titolare e all'eventuale esperto informatico o ditta incaricata nel caso sospetti o riscontri un problema di sicurezza relativamente al trattamento dei dati personali;
- assicurare che il trattamento dei dati all'interno dell'Associazione avvenga nel rispetto dei principi e delle disposizioni di cui al Capo II del GDPR, ed in particolare assicurare che:
  - i dati siano trattati in modo lecito, corretto e trasparente
  - i dati siano raccolti solo per le specifiche finalità del trattamento assegnato (**principio di limitazione delle finalità**)
  - i dati siano adeguati, pertinenti e non eccedenti rispetto alle finalità (**principio di minimizzazione dei dati**)
  - i dati siano esatti e se necessario aggiornati (**principio di esattezza dei dati**), predisponendo eventuali direttive in ordine al loro aggiornamento;
  - i dati siano conservati per un periodo non superiore a quello necessario al raggiungimento delle finalità del trattamento (**principio della limitazione della conservazione**), impartendo eventuali ulteriori istruzioni in ordine alla cancellazione o alla anonimizzazione/minimizzazione.
- organizzare la formazione degli Incaricati in materia di protezione dei dati personali;
- garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui è venuto a conoscenza;
- eseguire ogni altra istruzione che sia eventualmente impartita dal Titolare;

 adottare, per ogni operazione di trattamento svolta in prima persona, le misure di sicurezza a cui è tenuto ciascun Incaricato, che si specificano qui di seguito:

MISURE DI SICUREZZA

In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario:

- ❑ controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro;
- ❑ restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato;
- ❑ conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate;
- ❑ non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Titolare;
- ❑ laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro;
- ❑ qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili;
- ❑ custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente;
- ❑ prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;
- ❑ richiedere autorizzazione al Titolare per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali.

In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario:

- ❑ utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password);
- ❑ custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Titolare in caso di smarrimento o sottrazione;
- ❑ modificare la password fornita al primo accesso, e poi ogni 3 mesi;
- ❑ adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate;
- ❑ mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi;
- ❑ 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.),
- ❑ conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati;
- ❑ curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Titolare le segnalazioni di aggiornamento ricevute;
- ❑ non aprire e-mail o allegati dall'incerta o pericolosa provenienza e 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;
- ❑ evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet

Ulteriori compiti, modalità e istruzioni potranno essere specificati e integrati successivamente, anche in base agli ambiti di autorizzazione al trattamento corrispondenti alle credenziali di autenticazione assegnate all'Incaricato.

In relazione all'adempimento dei suoi compiti, il Responsabile interno propone al Titolare l'impiego di adeguate risorse umane, tecniche ed economiche.
Luogo e data _____

Per presa visione e accettazione
Il Responsabile interno/Referente del trattamento

_____

Il Titolare
Associazione _____
Il Presidente _____

_____

ATTO DI NOMINA A INCARICATO/AUTORIZZATO
AL TRATTAMENTO DEI DATI

L'associazione _____ (C.F. _____; tel. _____; fax _____; mail _____), con sede in _____, Titolare del trattamento ai sensi dell'art. 4 comma 1 n. 7 GDPR, in persona del Presidente e legale rappresentante _____

NOMINA

_____ (C.F. _____), nato/a a _____ in data _____, tel. _____, mail _____, cell. _____, che all'interno dell'Associazione ha la qualifica di _____ quale Persona autorizzata al trattamento dei dati personali ai sensi dell'art. 28 GDPR, di seguito indicato anche quale "Incaricato"

OPPURE

[CATEGORIA DI PERSONE ES. CONSIGLIERI, VOLONTARI, ECC.)
quali persone autorizzate al trattamento dei dati personali ai sensi dell'art. 28 GDPR, di seguito indicati anche quale "Incaricati"

AUTORIZZA

l'Incaricato a svolgere, all'interno dell'Associazione, le seguenti attività di trattamento dei dati, necessarie allo svolgimento delle mansioni e compiti relativi alla propria funzione/ruolo/attività, e relative alle seguenti finalità

- ✓ trattamento dei dati degli _____ al fine di _____;
- ✓ trattamento dei dati degli _____ al fine di _____;
- ✓ trattamento dei dati degli _____ al fine di _____;
- ✓ trattamento dei dati degli _____ al fine di _____;

[*in alternativa si può fare riferimento ai vari trattamenti descritti nel Registro delle attività di trattamento*]

FORNISCE ALL'INCARICATO LE SEGUENTI ISTRUZIONI

ISTRUZIONI E PRESCRIZIONI GENERALI

1. Trattare i dati esclusivamente per lo svolgimento delle mansioni e dei compiti assegnati.
2. Laddove sia compito dell'Incaricato raccogliere i dati presso l'interessato, consegnare o mostrare o trasmettere all'Interessato, all'atto della raccolta dei dati o, se raccolti presso terzi, all'atto della prima registrazione, l'informativa ai sensi dell'art. 13 comma 2 GDPR, salvo diverse indicazioni del Titolare o dell'eventuale Responsabile interno.
3. Laddove sia compito dell'Incaricato acquisire il consenso dell'Interessato nei casi previsti dall'art. 7, 8, 9 e 10 GDPR, far sottoscrivere l'autorizzazione/consenso previa lettura e/o consegna dell'informativa, salvo diverse indicazioni del Titolare o dell'eventuale Responsabile interno.
4. Trattare i dati nel rispetto dei principi e delle disposizioni di cui al Capo II del GDPR, ed in particolare:
   - trattare i dati in modo lecito, corretto e trasparente
   - raccogliere i dati solo per le specifiche finalità del trattamento assegnato (**principio di limitazione delle finalità**)
   - assicurare che i dati siano adeguati, pertinenti e non eccedenti rispetto alle finalità (**principio di minimizzazione dei dati**)
   - assicurare che i dati siano esatti e se necessario aggiornati (**principio di esattezza dei dati**), seguendo le eventuali ulteriori direttive del Titolare o dell'eventuale Responsabile interno in ordine al loro aggiornamento;
   - conservare i dati per un periodo non superiore a quello necessario al raggiungimento delle finalità del trattamento (**principio della limitazione della conservazione**), seguendo le eventuali ulteriori istruzioni del Titolare o dell'eventuale Responsabile interno in ordine alla cancellazione o alla anonimizzazione;
5. Comunicare e diffondere i dati esclusivamente ai soggetti indicati dal Titolare o dall'eventuale Responsabile interno, secondo le modalità stabilite nell'informativa e/o nel Registro dei Trattamenti.
6. Porre in essere tutte le attività e condotte dirette a garantire un'adeguata sicurezza dei dati, compresa la protezione da trattamenti non autorizzati o illeciti, e ad evitare la perdita, la distruzione o il danno accidentale (**principio di integrità e riservatezza**).
7. Inoltrare tempestivamente al Titolare o all'eventuale Responsabile interno o a _____ le richieste degli interessati volte all'esercizio dei diritti previsti dagli artt. 15, 16, 17, 18, 20, 21 GDPR.
8. Dare immediata comunicazione al Titolare e all'eventuale Responsabile interno e a _____ nel caso sospetti o riscontri un problema di sicurezza relativamente al trattamento dei dati personali.
9. Partecipare agli eventi formativi in materia di protezione dei dati personali.
10. Fornire collaborazione al Titolare e all'eventuale Responsabile interno per consentire a questi di svolgere correttamente la propria attività di direzione e controllo sulle operazioni di trattamento;
11. Garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui è venuto a conoscenza;
12. Eseguire ogni altra istruzione che sia eventualmente impartita dal Titolare o dall'eventuale Responsabile interno in occasioni specifiche.

MISURE DI SICUREZZA

In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario:

- ❑ controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro;
- ❑ restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato;
- ❑ conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate;
- ❑ non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Titolare o dell'eventuale Responsabile interno;
- ❑ laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro;
- ❑ qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili;
- ❑ custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente;
- ❑ prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;
- ❑ richiedere autorizzazione al Titolare o all'eventuale Responsabile interno per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali.

In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario:

- ❑ utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password);
- ❑ custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Titolare o all'eventuale Responsabile interno in caso di smarrimento o sottrazione;
- ❑ modificare la password fornita al primo accesso, e poi ogni 3 mesi;
- ❑ adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate;
- ❑ mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi;
- ❑ 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.),
- ❑ conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati;
- ❑ curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Titolare o all'eventuale Responsabile interno le segnalazioni di aggiornamento ricevute;
- ❑ non aprire e-mail o allegati dall'incerta o pericolosa provenienza e 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;
- ❑ evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet

Ulteriori compiti, modalità e istruzioni potranno essere specificati e integrati successivamente, anche in base agli ambiti di autorizzazione al trattamento corrispondenti alle credenziali di autenticazione assegnate all'Incaricato.

Luogo e data _____

Per presa visione e accettazione
L'Incaricato al trattamento

_____

Il Titolare
Associazione _____
Il Presidente _____

_____

ACCORDO INCARICO AL RESPONSABILE (ESTERNO) DEL TRATTAMENTO

ai sensi dell'art. 28 del Regolamento Europeo 2016/679 (in seguito anche "GDPR")

tra

l'associazione _____ (C.F. _____; tel. _____; fax _____; mail _____), con sede in _____, Titolare del trattamento ai sensi dell'art. 4 comma 1 n. 7 GDPR, in persona del Presidente e legale rappresentante _____

e

_____ (C.F. _____ - P.I. _____), con sede in _____, in persona del legale rappresentante _____, Responsabile del trattamento ai sensi dell'art. 28 GDPR

[*Oppure, in caso di persona fisica*]

_____ (C.F. _____ - P.I. _____), con sede in _____, Responsabile del trattamento ai sensi dell'art. 28 GDPR

premesso che

- in forza del contratto/incarico stipulato in data _____ (di seguito denominato il "Contratto"), il Titolare del trattamento si avvale di _____, per i servizi di _____ (di seguito, i "Servizi");
- l'espletamento dei Servizi comporta un trattamento di dati personali, come definiti all'art. 4 comma 1 GDPR, che _____ deve svolgere per conto del Titolare;
- il GDPR e il Codice impongono una serie di obblighi e vincoli al trattamento di dati personali da parte del Titolare, che anche il Responsabile è tenuto a rispettare;
- che _____ ha dimostrato di offrire garanzie sufficienti in ordine all'adozione di misure tecniche e organizzative adeguate per far sì che il trattamento dei dati sia conforme alle disposizioni del GDPR e sia idoneo alla tutela dei diritti dell'interessato;
- che con il presente accordo (di seguito l'"Accordo") il Titolare del trattamento intende dunque procedere alla nomina di _____ quale Responsabile del trattamento, impartendogli dettagliate istruzioni in relazione al trattamento dei dati.

Tutto ciò premesso si
conviene quanto segue

1. Nomina a Responsabile del trattamento

Con il presente Accordo il Titolare del trattamento _____ nomina, ai sensi dell'art. 28 GDPR, _____ quale Responsabile del trattamento dei dati, in relazione ai tutti i trattamenti di dati che sono necessari allo svolgimento dei Servizi di cui al Contratto.

2. Caratteristiche del trattamento

Il trattamento è consentito per tutto il tempo necessario all'esecuzione dei Servizi oggetto del Contratto ed è necessario in particolare al perseguimento delle seguenti finalità:

a) _____;
b) _____.

Il trattamento potrà avere ad oggetto dati personali comuni e, ove necessario, dati personali "particolari", e potrà essere svolto in via cartaceo o informatica.

3. Obblighi del Responsabile del trattamento

Il Responsabile del trattamento è tenuto, ai sensi dell'art. 28 terzo comma GDPR, a:

a) trattare i dati personali trasmessi dal Titolare o comunque acquisiti in relazione al Servizio da svolgere in corrispondenza alle istruzioni del Titolare e agli obblighi previsti dal presente Accordo, informando comunque immediatamente il Titolare qualora, a suo parere, un'istruzione impartita violi il GDPR o la normativa italiana sulla protezione dei dati;
b) individuare e nominare per iscritto le persone autorizzate al trattamento all'interno della propria struttura ("Incaricati") e garantire che i predetti Incaricati si impegnino alla riservatezza dei dati o abbiano un adeguato obbligo legale di riservatezza e si impegnino altresì all'adozione delle misure di sicurezza adottate e al rispetto dei principi del trattamento dei dati di cui al Capo II del GDPR;
c) adottare e descrivere al Titolare tutte le misure di sicurezza richieste dall'art. 32 GDPR, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
d) informare il Titolare della nomina di propri Responsabili al trattamento ("sub-Responsabili") nonché della loro successiva sostituzione con nuovi Responsabili, al fine di permettere al Titolare di valutare l'idoneità degli stessi ed eventualmente opporsi alla nomina o sostituzione. In caso di nomina autorizzata di altro Responsabile, a individuare le specifiche attività di trattamento del Responsabile e a stipulare con il Responsabile apposito contratto con il quale il Responsabile assuma, in relazione ai trattamenti svolti, gli stessi obblighi previsti nel presente Accordo;
e) collaborare con il Titolare, con misure tecniche e organizzative adeguate, ove possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato descritti negli artt. da 15 a 22 GDPR, con le modalità di cui all'art. 12 GDPR e le tempistiche indicate nell'art. 12 terzo comma GDPR. A tal fine, il Responsabile trasmette le eventuali richieste degli interessati, all'indirizzo mail del Titolare _____ entro 24 ore dal ricevimento della richiesta;

f) in relazione al trattamento svolto, assistere e collaborare con il Titolare ai fini del rispetto degli obblighi imposti al Titolare dagli artt. da 33 a 36 GDPR, ed in particolare:
   - informare il Titolare, senza ingiustificato ritardo, e comunque al più tardi entro 24 ore dal momento in cui ne è venuto a conoscenza, all'indirizzo mail del Titolare _____ di ogni violazione di dati personali, al fine di permettere al Titolare la notifica al Garante per la Protezione dei Dati Personali ai sensi dell'art. 33 GDPR e, se del caso, la comunicazione all'interessato ai sensi dell'art. 43 GDPR, fornendo tutte le informazioni sulla predetta violazione che siano a sua conoscenza tra quelle indicate dall'art. 33 comma 3 GDPR;
   - assistere e collaborare con il Titolare nel processo di eventuale valutazione d'impatto sulla protezione dei dati ("DPIA – Data Protection Impact Assessment"*)* di cui all'art. 35 GDPR, nonché nella eventuale fase di consultazione preventiva con l'Autorità di controllo ai sensi dell'art. 36 GDPR, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio;

g) cancellare o restituire tutti i dati personali una volta cessata in via definitiva l'esecuzione dei Servizi e cancellare le copie esistenti secondo le istruzioni ricevute dal Titolare, salvo che la conservazione dei dati sia prevista dal diritto dell'Unione o dalla normativa italiana;

h) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto, da parte del Responsabile, degli obblighi di cui al presente Accordo e contribuire alle attività di revisione, comprese le ispezioni, poste in essere dal Titolare.

Il Responsabile del trattamento è tenuto, ove sussistano le condizioni di cui all'art. 30 comma 5 GDPR, alla redazione e al costante aggiornamento di un "Registro delle attività di trattamento" svolte per conto del Titolare, in forma scritta, anche in formato elettronico, da tenere a disposizione in ogni momento del Titolare, con il contenuto di cui all'art. 30 comma2 GDPR.

Il Responsabile del trattamento è altresì tenuto:

- ove compia una autonoma valutazione d'impatto sulla protezione dei dati ("DPIA Data Protection Impact Assessment"*)* di cui all'art. 35 GDPR in relazione ai propri servizi, prodotti, asset che coinvolgano i trattamenti compiuti per conto del Titolare, a comunicare tempestivamente al Titolare il report finale della DPIA svolta;
- ad informare tempestivamente il Titolare qualora intenda avvalersi di servizi "Cloud" per il trattamento dei dati personali, assicurandosi altresì che i dati stessi vengano conservati all'interno dell'Unione Europea.

Il Responsabile si impegna altresì a valutare, ai fini della dimostrazione della propria idoneità all'incarico, l'adesione ad eventuali codici di condotta o ad un meccanismo di certificazione approvati ai sensi dell'art. 40 e 42 GDPR.

4. Principi del trattamento dei dati

Il Responsabile del trattamento è tenuto, in relazione a tutti i trattamenti svolti per conto del Titolare, al rispetto dei principi di cui al Capo II del GDPR, nonché a consentire al Titolare di poter dimostrarne il rispetto nei confronti degli interessati e del Garante per la Protezione dei dati personali.

A titolo esemplificativo e non esaustivo si precisa che i dati:

- devono essere trattati in modo lecito, corretto e trasparente;
- devono essere raccolti solo per le finalità del trattamento, svolto dal Responsabile, che siano determinate, esplicite e legittime;
- devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità;
- devono essere esatti e se necessario aggiornati;
- devono essere conservati per un periodo non superiore a quello necessario al raggiungimento delle finalità del trattamento. Trascorso detto periodo i dati vanno resi anonimi o cancellati;
- se comuni vanno trattati nei casi indicati all'art. 6 GDPR;
- se "particolari" vanno trattati nei casi indicati dall'art. 9 e 10 GDPR.

Il Responsabile è altresì tenuto al rispetto degli obblighi di informativa all'interessato ai sensi dell'art. 13 comma 2 GDPR e di acquisizione del consenso nei casi previsti dall'art. 7, 8, 9 e 10 GDPR, nonché a garantire all'interessato, in relazione ai trattamenti svolti per conto del Titolare, l'esercizio dei diritti previsti dagli artt. 15, 16, 17, 18, 20, 21 GDPR.

Il Responsabile è comunque tenuto e ha il potere di svolgere ogni incombenza connessa all'esecuzione dell'incarico di cui al presente Accordo che sia necessaria o opportuna per l'esercizio dei compiti indicati nel presente Accordo.

5. Disposizioni generali e finali

Le Parti dichiarano di aver letto e pienamente compreso il contenuto del presente Accordo e di esprimere pienamente, con la sottoscrizione, il loro consenso. Eventuali modifiche al presente Accordo, se del caso anche mediante l'inserimento di "clausole tipo" di cui all'art. 28 comma 6 GDPR, dovranno essere apportate esclusivamente per iscritto.

L'invalidità, anche parziale, di una o più delle clausole del presente Accordo non pregiudica la validità delle restanti clausole.

L'incarico di Responsabile del trattamento dei dati è di carattere fiduciario e non è quindi suscettibile di delega, salva la nomina di sub-responsabili ai sensi del presente Accordo. L'incarico di Responsabile del Trattamento cessa automaticamente alla scadenza o alla cessazione del Contratto e/o del Servizi affidati, salvi gli obblighi attinenti al trattamento dei dati da considerarsi esistenti anche successivamente alla cessazione del rapporto.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni in materia di protezione dei dati personali di cui al GDPR e al D.Lgs. n. 196 del 29.7.2003 (Codice in materia di protezione dei dati personali).

Per accettazione dell'incarico
Il Responsabile del trattamento
_____

_____

Il Titolare
Associazione _____
Il Presidente _____

_____

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO EX ART. 30 GDPR DEL TITOLARE ASSOCIAZIONE _____	
Codice Fiscale	
Iscrizione Registri	
Indirizzo SEDE	
Nr. di telefono	
Indirizzo e-mail	
Indirizzo PEC	
DATA PROTECTION OFFICER	
EVENTUALI CONTITOLARI	

_____, _____

Il Presidente

descrizione sintetica del trattamento	**1. TRATTAMENTO DEI DATI DEGLI ASPIRANTI SOCI E DEI SOCI**
ev. Contitolare	
categorie di interessati	chiunque presenta domanda di adesione soci/aderenti/volontari *aspiranti soci e soci minorenni*
categorie di dati personali	**dati personali comuni** (dati anagrafici, C.F., riferimenti telefonici, e-mail, residenza, percorso di studi o condizione professionale) **immagini fotografiche o video** dei Volontari
finalità del trattamento	per la gestione del rapporto associativo (invio della corrispondenza, convocazione alle sedute degli organi, procedure amministrative interne) e per l'organizzazione ed esecuzione del servizio per adempiere agli obblighi di legge (es. fiscali, assicurativi, ecc.) riferiti ai soci dell'Associazione; per l'invio (tramite posta, posta elettronica, newsletter o numero di cellulare o altri mezzi informatici) di comunicazioni legate all'attività e iniziative dell'Associazione *in relazione alle immagini/video, per la pubblicazione sul sito dell'Associazione, sulla pagina FB o i social network dell'Associazione o su newsletter o su materiale cartaceo di promozione delle attività istituzionali dell'Associazione* *in relazione alla foto personale, per l'inserimento nel tesserino di riconoscimento* per la partecipazione dei soci a corsi, incontri e iniziative e per l'organizzazione e gestione dei corsi per analisi statistiche, anche in forma aggregata.
base giuridica del trattamento	richiesta di adesione e contratto associativo (art. 6 comma 1 lett. b GDPR) consenso al trattamento (art. 6 comma 1 lett. a – art. 9 comma 2 lett. a GDPR) contatti regolari con l'Associazione (art. 9 comma 2 lett. d GDPR) obblighi legali a cui è tenuta l'Associazione (art. 6 comma 1 lett. c GDPR)
modalità di acquisizione dei dati	I dati vengono acquisiti: *per un primo contatto, compilando un **form sul sito dell'Associazione** (nome, cognome, telefono, sesso e mail)* compilando la **DOMANDA DI ISCRIZIONE** cartacea presso la sede. *nome, cognome e CF vengono trasmessi/confermati dal socio anche in sede di iscrizione al singolo corso.*
modalità di Informativa e acquisizione del consenso	*in occasione del primo contatto nel sito dell'Associazione l'informativa è visibile mediante link accanto al form di primo contatto →* ***INFORMATIVA PRIMO CONTATTO*** informativa e consenso al trattamento sono riportate nel retro della domanda di iscrizione (a socio) cartacea e sono quindi visionate e sottoscritte dall'aspirante socio al momento della presentazione della domanda → **INFORMATIVA E CONSENSO PER SOCI** → **INFORMATIVA E CONSENSO PER SOCI MINORENNI**
dove sono conservati i dati	la DOMANDA DI ISCRIZIONE cartacea è conservata presso la sede. I dati vengono inseriti nel Libro Soci e nei sistemi informatici dell'Associazione
ev. Responsabile interno del trattamento	
Incaricati	Gli incaricati o le categorie di Incaricati che trattano i dati sono *indicati nell'**ALLEGATO 1 foglio A***
Categoria dei destinatari o destinatari a cui possono essere comunicati i dati. Eventuali Responsabili (esterni) del Trattamento. Diffusione dei dati	I dati dei soci/donatori vengono trasmessi: *agli altri soci ai sensi di statuto, per l'organizzazione ed esecuzione del servizio, limitatamente a _____* ai soggetti deputati allo svolgimento di attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, assicuratore, sistemista, ecc.) a tutte le persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale allo svolgimento dell'attività istituzionale (formatori, Enti Locali, ditte che curano la manutenzione informatica, società organizzatrici dei corsi, ecc.). *Detti soggetti sono indicati nell'**ALLEGATO 1 foglio B**, con precisazione se sono stati nominati Responsabili esterni del trattamento ai sensi dell'art. 28 GDPR.* I dati non sono trasferiti a destinatari con sede extra UE. [*oppure*] I dati sono trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali o previa verifica che il destinatario garantisca adeguate misure di protezione. *Previo consenso del socio, vengono diffuse mediante il sito dell'Associazione, i social network dell'Associazione, la newsletter o materiale cartaceo immagini/video raffiguranti i soci in occasioni ed eventi istituzionali*
termine ultimo per la cancellazione	ove la persona non diventi socio, i dati sono conservati (limitatamente a nome e cognome ed esito della valutazione di idoneità) ai soli fini storici e statistici e al fine di conservare traccia della richiesta di adesione il trattamento dei dati per la gestione del rapporto associativo viene svolto fino alla cessazione del rapporto associativo dopo la cessazione del rapporto associativo, i dati relativi a _____ vengono conservati per finalità di archivio, obblighi legali o contabili o fiscali o per esigenze di tutela dell'Associazione, con esclusione di comunicazioni a terzi e diffusione
misure di sicurezza informatiche	*Accesso a computer e gestionali tramite autenticazione con nome utente e password; utilizzo firewall e antivirus di protezione; aggiornamenti del sistema operativo; utilizzo programma per backup giornaliero.* *Per la descrizione specifica del sistema hardware e software si veda **ALLEGATO 1 foglio C***
misure di sicurezza organizzative	*Gli archivi cartacei sono custoditi in armadi, uffici e archivi chiusi a chiave e a cui può accedere solo il personale incaricato dall'Associazione*
possibili rischi e misure adottate o da adottarsi per limitare i rischi	

descrizione sintetica del trattamento	**2. TRATTAMENTO DEI DATI DEI BENEFICIARI/UTENTI DEL SERVIZIO E DEGLI ESTERNI PARTECIPANTI A CORSI, SEMINARI ED EVENTI**
ev. Contitolare	
categorie di interessati	utenti / beneficiari del servizio ed in particolare _____ utenti / beneficiari del servizio minorenni ed in particolare _____ chiunque (non socio) presenta domanda di frequenza ai corsi, convegni e seminari e di partecipazione ed eventi associativi
categorie di dati personali	**dati personali comuni** (dati anagrafici, C.F., riferimenti telefonici, e-mail, residenza, coordinate bancarie ed eventuali altri dati indicati nei documenti fiscali) ***dati sanitari*** *(_____)* ***dati giudiziari*** *(.....)* *immagini fotografiche o video dei partecipanti*
finalità del trattamento	l'esecuzione della richiesta o del servizio richiesto e la gestione dell'eventuale contratto l'organizzazione e gestione dei corsi, convegni, seminari ed eventi associativi e invio ai partecipanti informazioni su successive iniziative formative dell'Associazione analisi statistiche, anche in forma aggregata adempimento dei relativi obblighi di legge
base giuridica del trattamento	contratto o richiesta di servizio (art. 6 comma 1 lett. b GDPR) obbligo legale (art. 6 comma 1 lett. c GDPR) consenso al trattamento (art. 6 comma 1 lett. a – art. 9 comma 2 lett. a GDPR)
modalità di acquisizione dei dati	I dati personali sono raccolti al momento della stipula del contratto e/o fornitura di beni e servizi o della domanda di partecipazione agli eventi e corsi
modalità di Informativa e acquisizione del consenso	L'informativa è resa al momento della richiesta di servizio e/o della stipula del contratto oppure è riportata (insieme alla richiesta di consenso al trattamento) nel retro della domanda di partecipazione ai corsi, convegni, seminari ed eventi associativi → **INFORMATIVA E CONSENSO BENEFICIARI ED ESTERNI** → **INFORMATIVA E CONSENSO BENEFICIARI ED ESTERNI MINORENNI**
dove sono conservati i dati	in cartaceo presso la sede nei sistemi informatici dell'Associazione
ev. Responsabile interno del trattamento	
Incaricati	Gli incaricati o le categorie di Incaricati che trattano i dati sono *indicati nell'**ALLEGATO 1 foglio A***
Categoria dei destinatari o destinatari a cui possono essere comunicati i dati. Eventuali Responsabili (esterni) del Trattamento. Diffusione dei dati	I dati potranno essere comunicati ai soggetti deputati allo svolgimento dei servizi e attività richieste (es. formatori esterni) e alle attività a cui l'Associazione è tenuta in base ad obbligo di legge (commercialista, assicuratore, sistemista, ecc.). *Detti soggetti sono indicati nell'**ALLEGATO 1 foglio B**, con precisazione se sono stati nominati Responsabili esterni del trattamento ai sensi dell'art. 28 GDPR.* I dati non sono trasferiti a destinatari con sede extra UE. [*oppure*] I dati sono trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali o previa verifica che il destinatario garantisca adeguate misure di protezione. *Previo consenso dell'utente/beneficiario, vengono diffuse mediante il sito dell'Associazione, i social network dell'Associazione, la newsletter o materiale cartaceo immagini/video raffiguranti la persona in occasione dei corsi ed eventi cui partecipa*
termine ultimo per la cancellazione	I dati degli utenti/beneficiari vengono trattati per il tempo necessario all'esecuzione del servizio, e successivamente solo in relazione agli obblighi legali o contabili o fiscali o per esigenze di tutela legale dell'Associazione I dati dei partecipanti a corsi, convegni e seminari ed eventi associativi vengono cancellati una volta svolto l'evento, salva la conservazione in forma anonima per fini statistici e di archivio e salvo l'inserimento nella newsletter previo consenso
misure di sicurezza informatiche	*Accesso a computer e gestionali tramite autenticazione con nome utente e password; utilizzo firewall e antivirus di protezione; aggiornamenti del sistema operativo; utilizzo programma per backup giornaliero.* *Per la descrizione specifica del sistema hardware e software si veda **ALLEGATO 1 foglio C***
misure di sicurezza organizzative	*Gli archivi cartacei sono custoditi in armadi, uffici e archivi chiusi a chiave e a cui può accedere solo il personale incaricato dall'Associazione*
possibili rischi e misure per misure adottate o da adottarsi per limitare i rischi	

descrizione sintetica del trattamento	**3. TRATTAMENTO DEI DATI DEI CONSULENTI, COLLABORATORI E FORNITORI ESTERNI**
ev. Contitolare	
categorie di interessati	consulenti e collaboratori esterni dell'Associazione (commercialisti, consulenti del lavoro, notai, amministratori di sistema o gestore dei sistemi informatici, ecc.) fornitori di beni e servizi
categorie di dati personali	**dati personali comuni** (ragione sociale, C.F., partita IVA, indirizzo della sede legale, e-mail, recapiti telefonici, coordinate bancarie ed eventuali altri dati indicati nei documenti fiscali o nei contratti/convenzioni)
finalità del trattamento	gestione dell'eventuale contratto/convenzione o rapporto adempimento dei relativi obblighi di legge
base giuridica del trattamento	contratto di servizio (art. 6 comma 1 lett. b GDPR) obbligo legale (art. 6 comma 1 lett. c GDPR) consenso al trattamento (art. 6 comma 1 lett. a – art. 9 comma 2 lett. a GDPR)
modalità di acquisizione dei dati	I dati personali sono raccolti al momento della stipula del contratto di consulenza o di collaborazione o di fornitura
modalità di Informativa e acquisizione del consenso	L'informativa → **INFORMATIVA CONSULENTI, COLLABORATORI E FORNITORI** è resa al momento della stipula del contratto di fornitura e (se esiste) dell' → **ACCORDO/INCARICO A RESPONSABILE ESTERNO**. *Non è necessario il consenso*
dove sono conservati i dati	in cartaceo presso la sede nei sistemi informatici dell'Associazione
ev. Responsabile interno del trattamento	
Incaricati	Gli incaricati o le categorie di Incaricati che trattano i dati sono *indicati nell'**ALLEGATO 1 foglio A***
Categoria dei destinatari o destinatari a cui possono essere comunicati i dati. Eventuali Responsabili (esterni) del Trattamento. Diffusione dei dati	I dati sono comunicati a soggetti pubblici e privati per adempiere agli specifici obblighi di legge derivanti dal contratto di consulenza, collaborazione e fornitura. I dati non vengono diffusi.
termine ultimo per la cancellazione	I dati sono trattati per tutta la durata del contratto/rapporto in essere e, successivamente, e successivamente solo in relazione agli obblighi legali o contabili o fiscali o per esigenze di tutela legale dell'Associazione
misure di sicurezza informatiche	*Accesso a computer e gestionali tramite autenticazione con nome utente e password; utilizzo firewall e antivirus di protezione; aggiornamenti del sistema operativo; utilizzo programma per backup giornaliero.* *Per la descrizione specifica del sistema hardware e software si veda **ALLEGATO 1 foglio C***
misure di sicurezza organizzative	*Gli archivi cartacei sono custoditi in armadi, uffici e archivi chiusi a chiave e a cui può accedere solo il personale incaricato dall'Associazione*
possibili rischi e misure per misure adottate o da adottarsi per limitare i rischi	

descrizione sintetica del trattamento	**4. TRATTAMENTO DEI DATI DEI DIPENDENTI**
ev. Contitolare	
categorie di interessati	Dipendenti dell'Associazione
categorie di dati personali	**dati personali comuni** (dati anagrafici, C.F., indirizzo di residenza, e-mail, recapiti telefonici, inquadramento contrattuale, retribuzione, coordinate bancarie e altre informazioni fornite dall'interessato attraverso il curriculum vitae) **dati relativi alla salute** immagini e video
finalità del trattamento	gestione del rapporto di lavoro e adempimento degli obblighi di legge e di contratto
base giuridica del trattamento	contratto di lavoro (art. 6 comma 1 lett. b e art. 9 comma 2 lett. b GDPR) obbligo legale (art. 6 comma 1 lett. c GDPR) consenso al trattamento (art. 6 comma 1 lett. a – art. 9 comma 2 lett. a GDPR)
modalità di acquisizione dei dati	I dati personali sono raccolti attraverso la candidatura al ruolo ricoperto e la presentazione del curriculum o al momento della stipula del contratto di lavoro
modalità di Informativa e acquisizione del consenso	L'informativa è resa all'atto della stipula del contratto di lavoro → **INFORMATIVA PER I DIPENDENTI** Il consenso è necessario solo per la diffusione del cognome, nome, ruolo, immagine nel sito web ed è acquisito mediante la sottoscrizione alla fine dell'informativa → **INFORMATIVA E CONSENSO PERI DIPENDENTI**
dove sono conservati i dati	in cartaceo presso la sede nei sistemi informatici dell'Associazione
ev. Responsabile interno del trattamento	
Incaricati	Gli incaricati o le categorie di Incaricati che trattano i dati sono *indicati nell'**ALLEGATO 1 foglio A***
Categoria dei destinatari o destinatari a cui possono essere comunicati i dati. Eventuali Responsabili (esterni) del Trattamento. Diffusione dei dati	I dati sono comunicati a soggetti pubblici e privati (INPS, INAIL, commercialista, consulente del lavoro, RSPP, studio medico) competenti per l'esecuzione di servizi necessari per una corretta gestione del rapporto di lavoro. *I dati relativi a nome e cognome, al ruolo ricoperto e l'immagine possono essere diffusi, previo consenso, attraverso il sito istituzionale, i social network e sul materiale informativo cartaceo dell'Associazione*. I dati relativi allo stato di salute non sono diffusi o comunicati a terzi e sono trattati unicamente dall'Associazione e dal medico competente.
termine ultimo per la cancellazione	I dati sono trattati per tutta la durata del contratto/rapporto in essere e, successivamente, e successivamente solo in relazione agli obblighi legali o contabili o fiscali o per esigenze di tutela legale dell'Associazione
misure di sicurezza informatiche	*Accesso a computer e gestionali tramite autenticazione con nome utente e password; utilizzo firewall e antivirus di protezione; aggiornamenti del sistema operativo; utilizzo programma per backup giornaliero.* *Per la descrizione specifica del sistema hardware e software si veda **ALLEGATO 1 foglio C***
misure di sicurezza organizzative	*Gli archivi cartacei sono custoditi in armadi, uffici e archivi chiusi a chiave e a cui può accedere solo il personale incaricato dall'Associazione*
possibili rischi e misure per misure adottate o da adottarsi per limitare i rischi	

descrizione sintetica del trattamento	**5. TRATTAMENTO DEI DATI DEGLI UTENTI DEL SITO ISTITUZIONALE**
ev. Contitolare	
categorie di interessati	Chiunque naviga sul sito istituzionale *(per chi compila i form esistenti nel sito si rinvia alla descrizione del trattamento relativo al servizio per cui viene compilato il form)*
categorie di dati personali	**dati di navigazione** (cookies)
finalità del trattamento	*miglioramento della navigazione e maggiore funzionalità del sito web, raccolta di informazioni statistiche aggregate sull'utilizzo del sito da parte degli utenti (numero di visitatori, pagine visitate, tempo di permanenza, parole chiave, ecc.) attraverso programmi come Shinystat, Google Analytics, Awstats*
base giuridica del trattamento	legittimo interesse del titolare (art. 6 comma 1 lett. f GDPR)
modalità di acquisizione dei dati	*I dati vengono acquisiti tramite programmi come Shinystat, Google Analytics, Awstats*
modalità di Informativa e acquisizione del consenso	L'informativa è resa disponibile nell'home page del sito istituzionale → **INFORMATIVA PER UTENTI DEL SITO WEB** Il consenso non è acquisito in quanto non necessario
dove sono conservati i dati	I server che ospitano le pagine del sito web sono presso _____
ev. Responsabile interno del trattamento	
Incaricati	Gli incaricati o le categorie di Incaricati che trattano i dati sono *indicati nell'**ALLEGATO 1 foglio A***
Categoria dei destinatari o destinatari a cui possono essere comunicati i dati. Eventuali Responsabili (esterni) del Trattamento. Diffusione dei dati	I dati possono essere conosciuti dalla ditta che gestisce il sito internet e dalla ditta incaricata della manutenzione tecnico – informatica *Detti soggetti sono indicati nell'**ALLEGATO 1 foglio B**, con precisazione se sono stati nominati Responsabili esterni del trattamento ai sensi dell'art. 28 GDPR.* I dati non sono trasferiti a destinatari con sede extra UE. [*oppure*] I dati sono trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali o previa verifica che il destinatario garantisca adeguate misure di protezione
termine ultimo per la cancellazione	
misure di sicurezza informatiche	*Accesso a computer e gestionali tramite autenticazione con nome utente e password; utilizzo firewall e antivirus di protezione; aggiornamenti del sistema operativo; utilizzo programma per backup giornaliero*
misure di sicurezza organizzative	
possibili rischi e misure per misure adottate o da adottarsi per limitare i rischi	Accesso ai locali consentito solo a persone autorizzate. Locali protetti da sistema di allarme e ingressi videosorvegliati.

descrizione sintetica del trattamento	**6. TRATTAMENTO DEI DATI DEGLI ISCRITTI ALLA NEWSLETTER**
ev. Contitolare	
categorie di interessati	chi si iscrive alla newsletter compilando il form presente sul sito istituzionale chi dà il consenso ad essere inserito nella newsletter i soci/aderenti
categorie di dati personali	nome, cognome e indirizzo e-mail
finalità del trattamento	invio della newsletter periodica sulle iniziative e attività dell'Associazione, ivi incluse eventuali campagne di sensibilizzazione e raccolta fondi
base giuridica del trattamento	contratto o richiesta di servizio (art. 6 comma 1 lett. b GDPR) consenso al trattamento (art. 6 comma 1 lett. a – art. 9 comma 2 lett. a GDPR) contatti regolari con l'Associazione (art. 9 comma 2 lett. d GDPR)
modalità di acquisizione dei dati	compilazione dell'apposito form presente sul sito istituzionale consenso all'iscrizione manifestato in occasione della domanda di partecipazione a corsi, seminari, eventi domanda di iscrizione a socio
modalità di Informativa e acquisizione del consenso	L'informativa è resa disponibile accanto al form di iscrizione ed è consegnata al momento della richiesta orale o cartacea → **INFORMATIVA PER ISCRITTI ALLA NEWSLETTER**
dove sono conservati i dati	
ev. Responsabile interno del trattamento	
Incaricati	Gli incaricati o le categorie di Incaricati che trattano i dati sono *indicati nell'**ALLEGATO 1 foglio A***
Categoria dei destinatari o destinatari a cui possono essere comunicati i dati. Eventuali Responsabili (esterni) del Trattamento. Diffusione dei dati	I dati possono essere conosciuti dalla ditta che gestisce la newsletter e dalla ditta incaricata della manutenzione degli strumenti informatrici dell'Associazione *Detti soggetti sono indicati nell'**ALLEGATO 1 foglio B**, con precisazione se sono stati nominati Responsabili esterni del trattamento ai sensi dell'art. 28 GDPR.* I dati non sono trasferiti a destinatari con sede extra UE. [*oppure*] I dati sono trasferiti a destinatari con sede extra UE in Stati che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali o previa verifica che il destinatario garantisca adeguate misure di protezione
termine ultimo per la cancellazione	I dati verranno utilizzati fino alla richiesta di cancellazione dalla newsletter, dopodiché verranno cancellati *(la cancellazione è automatica ove la persona intervenga direttamente sul portale)*
misure di sicurezza informatiche	*Accesso a computer e gestionali tramite autenticazione con nome utente e password; utilizzo firewall e antivirus di protezione; aggiornamenti del sistema operativo; utilizzo programma per backup giornaliero*
misure di sicurezza organizzative	
possibili rischi e misure per misure adottate o da adottarsi per limitare i rischi	