Corpo Nazionale Giovani Esploratori ed Esploratrici Italiani
Associazione di Promozione Sociale (ed) Ente Morale
sotto l'Alto Patronato del Presidente della Repubblica

membro degli organismi internazionali

VADEMECUM GDPR

Regolamento Europeo in materia di Protezione dei Dati Personali (2016/679)

Versione 1 del 24/11/2018

CF: 80149370589
Sede Centrale:
V.le di Val Fiorita n.88
1° Piano int. 7 - 00144 Roma

t +39 06 54221391
f +39 06 54210012
sc@cngei.it
www.cngei.it

Social:
facebook.com/cngei.it
twitter.com/cngei
instagram.com/cngei

INTRODUZIONE

Il 25 maggio 2018 è entrato definitivamente in vigore il Regolamento Europeo in materia di Protezione dei Dati Personali (2016/679) (in breve "GDPR"). Il Regolamento si applica anche alle organizzazioni di volontariato e gli Enti del Terzo Settore, che sono chiamate ad adeguare il loro sistema privacy e le misure di protezione dei dati alle novità introdotte dal Regolamento.
CNGEI ha ritenuto fondamentale analizzare approfonditamente il proprio sistema di trattamento dati, anche al fine di individuare i rischi maggiori soprattutto in relazione ai trattamenti di dati particolarmente delicati (i vecchi "dati sensibili").
L'analisi effettuata ha portato all'individuazione di una politica della privacy che, attraverso il presente vademecum pratico viene estesa a tutti i membri e a tutte le sezioni territoriali.
L'attenzione al progressivo evolversi delle fonti giuridiche ci permetterà di aggiornare periodicamente, qualora fosse necessario, il presente documento.

IL NUOVO REGOLAMENTO EUROPEO UE 2016/679 ("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).
In particolare, il GDPR, in termini non molto diversi dal "vecchio" Codice Privacy (D.Lgs. n. 196/2003), si propone di far sì:

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

La nostra Associazione, intesa nel suo complesso, raccoglie ed utilizza comunemente, nello svolgimento della propria attività, dati personali, e cioè informazioni e notizie riferite:

- ai propri iscritti beneficiari dell'attività istituzionale;
- ai consulenti e collaboratori esterni;
- ai dipendenti;
- ai soggetti "esterni" (enti pubblici, fornitori, altre associazioni) con particolare riferimento alle persone fisiche che ci lavorano o che con questi collaborano, nell'interfacciarsi con la nostra organizzazione.

Per ciò che concerne la natura dei dati, questi si distinguono in:

- dati comuni (ad esempio il nominativo, la data di nascita, il numero di cellulare degli iscritti, l'avvenuto versamento della quota associativa etc.);
- dati particolari, che comprendono i dati sanitari (i "vecchi" dati sensibili);

Sono dati personali, a cui si applicano le regole del GDPR implementate da CNGEI, anche le immagini, i suoni, i video ecc., quando consentono di individuare una persona determinata.

CNGEI QUALE TITOLARE DEL TRATTAMENTO

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

- che le decisioni sui trattamenti da svolgere vanno adottate dall'organo o dalle persone fisiche cui è attribuita la gestione dell'ente (es. Consiglio

Direttivo, il Presidente, ecc.);

- che gli adempimenti richiesti dal GDPR devono ovviamente essere attuati da persone fisiche (ad es. il Presidente, un consigliere delegato, i dipendenti, o anche i volontari);
- che i limiti imposti dal GDPR vanno rispettati da chiunque dell'associazione utilizzi dati personali;
- che, infine, le responsabilità civili, amministrative e penali in caso di violazione del GDPR gravano prevalentemente sulle persone fisiche che hanno agito.

Posto che per il GDPR il Titolare è la persona giuridica che decide che trattamento di dati svolgere e come svolgerlo ("determina le finalità e i mezzi del trattamento di dati personali"), i soggetti che operano all'interno dell'organizzazione, come sopra descritto a titolo esemplificativo, sono formalmente autorizzati ai trattamenti in coerenza con i ruoli assunti.
Le Sezioni locali, che operano "per conto" dell'associazione, nelle filiere di trattamento collegate alle attività istituzionali, assumono il ruolo di Responsabili Esterni, come espressamente previsto dal GDPR.
Laddove la stessa sezione eserciti un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, per esempio nel trattamento dei dati dei propri dipendenti e collaboratori, nella gestione del rapporto di lavoro, va considerata titolare del trattamento cioè soggetto autonomo ai fini dell'applicazione del GDPR e del rispetto degli obblighi conseguenti.

I CRITERI, I LIMITI E LE FINALITÀ CON CUI LE ASSOCIAZIONI DEVONO TRATTARE I DATI PERSONALI

Ai sensi dell'art. 5 del GDPR, CNGEI in qualità di Titolare del Trattamento e le sezioni locali, quali Responsabili Esterni:

- 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 rappresenta 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.
Nel CNGEI le finalità del trattamento dei dati coincidono con gli scopi istituzionali indicati nello statuto e vengono declinate nelle singole informative redatte per i soggetti di cui si gestiscono i dati.

Quindi ad esempio quando l'associazione raccoglie i dati comuni degli iscritti per gestire le attività istituzionali, non potrà, senza l'autorizzazione specifica degli stessi ("consenso informato") usare tali dati per scopi diversi: ad esempio non potrà comunicare il nome e l'indirizzo o altre informazioni a terzi per pubblicità, iniziative commerciali o comunque per scopi che non riguardano l'ente.

L'INFORMATIVA

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.
L'informativa deve contenere una serie di informazioni così come specificato nell'articolo 13 del GDPR (cui rimandiamo per i dettagli), tra cui vogliamo qui sottolineare:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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;
- qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- 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;

L'informativa per gli iscritti è stata redatta da CNGEI e messa a disposizione delle sezioni che avranno cura di renderla ai soggetti interessati, raccogliendo i dovuti consensi indicati nella stessa, laddove necessario.
L'informativa è rinvenibile nell'allegato nr 25 al Regolamento Nazionale (Allegato N° 25 - Informativa sul trattamento dei dati personali, ai sensi dell'articolo 13 GDPR 679_2016).
Operativamente:

- l'informativa (di cui all'allegato 25 al regolamento) va resa all'atto dell'iscrizione, cioè 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.
- 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 viene resa anche ai collaboratori esterni, ai dipendenti e a tutti coloro di cui CNGEI acquisisce, conserva e utilizza dati personali, che si possono definire "interessati". Ovviamente, in questo caso, l'informativa da utilizzare non sarà quella di cui sopra, ma altro modulo appositamente predisposto.
Laddove questi soggetti siano dipendenti, collaboratori o altro della singola sezione, sarà compito di questa, quale Autonomo Titolare di questi trattamenti di dati, rendere opportuna informativa al singolo soggetto interessato.

AGGIORNAMENTO E CONSERVAZIONE DEI DATI, ANCHE AL TERMINE DEL RAPPORTO ASSOCIATIVO

L'aggiornamento o la rettifica dei dati (art. 16 GDPR) deve essere svolta quando è necessario per il corretto raggiungimento delle finalità del trattamento o per soddisfare una legittima esigenza dell'interessato, anche perché rappresenta uno dei suoi diritti garantiti da GDPR.
E' interesse di CNGEI 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). Queste operazioni solitamente avvengono per il tramite della Sezione locale cui vengono trasferite alcune operazioni, dettagliate in apposito atto con cui vengono nominate quale Responsabili esterni al trattamento dei dati.
Per quanto concerne la conservazione e l'utilizzo dei dati personali degli iscritti anche dopo che essi hanno lasciato l'associazione (anche solo per conservare traccia di coloro che hanno "transitato" all'interno dell'ente), occorre sottolineare che l'art. 9 comma 2 lett. d) del GDPR consente l'utilizzo dei dati degli ex soci anche senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'associazione e con adeguate garanzie (di protezione dei dati), con divieto però di comunicazione all'esterno (per tale comunicazione ci vuole il consenso specifico dell'ex socio).
In applicazione del principio di proporzionalità e minimizzazione dei dati, i dati "trattenuti" dall'associazione dopo l'uscita del socio dovranno però essere strettamente inerenti alle specifiche attività "residue" (es. invio della newsletter ecc.), e quindi potranno per esempio ridursi al nominativo e all'indirizzo mail.

I DIRITTI DEGLI INTERESSATI

La protezione dei dati è assicurata all'interessato anche attraverso l'esercizio dei diritti indicati dagli articoli da 15 a 22 del GDPR.
Ogni persona può chiedere ad ogni titolare se e in che modo utilizza i suoi dati personali e può esercitare i diritti come di seguito elencato
In base agli articoli sopra citati l'interessato può infatti chiedere a CNGEI:

- 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 CNGEI 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).

CNGEI, quale titolare, potrebbe ricevere tale richiesta, anche per il tramite delle sezioni territoriali, in questi casi occorrerà immediatamente girare la richiesta alla Sede Centrale, che provvederà ad evaderla rispondendo all'interessato.

DAI DATI SENSIBILI AI DATI PARTICOLARI

Il GDPR contiene, all'art. 9, la definizione di "categorie particolari di dati personali" (più generica di quella che il Codice Privacy riservava ai sati sensibili), 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.
CNGEI gestisce dati "particolari" (sensibili) nello svolgimento delle proprie attività istituzionali e ha attuato le misure adeguate al fine di garantirne la tutela e la sicurezza.

LA GESTIONE DEI CONSENSI

Affinché sia valido il consenso deve avere le seguenti caratteristiche, come specificato all'art. 7 del GDPR:

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

dei trattamenti svolti in precedenza).

CNGEI ha l'obbligo di "essere in grado di dimostrare" di aver ottenuto il consenso, quando questo è necessario, dunque il consenso viene richiesto in forma scritta attraverso la sottoscrizione dell'interessato anche al fine di conservare prova dell'avvenuta autorizzazione.
Con riferimento agli interessati minorenni, il consenso va prestato da coloro che esercitano la responsabilità genitoriale o, se esiste, dal tutore.
La richiesta di autorizzazione/consenso va fatta sottoscrivere personalmente all'interessato e deve essere preceduta dall'informativa di cui all'art. 13 del GDPR e dal punto di vista operativo valgono le indicazioni già espresse per l'informativa.

Il DPO – Data Protection Officer

L'art. 37 del GDPR ha introdotto la nuova figura, del "Responsabile della Protezione dei Dati" (DPO) non prevista dal Codice Privacy.
Sono tenuti alla nomina del DPO solo gli Enti del Terzo Settore che, nello svolgimento della loro attività principale, svolgono un monitoraggio sistematico su larga scala dei beneficiari/destinatari della loro attività o compiono un trattamento su larga scala di dati particolari/sensibili o giudiziari.
Per determinare quando un trattamento di dati è svolto "su larga scala" si possono usare criteri quantitativi e qualitativi (numero degli interessati, numero di dati, estensione temporale e geografica del trattamento). Le linee guida europee (article 29 data protection working party) hanno indicato, a titolo esemplificativo, alcuni soggetti che svolgono trattamenti su vasta scala tra cui gli ospedali, le aziende di trasporto, le compagnie assicurative e gli istituti di credito, i fornitori di servizi di telecomunicazione, ecc.
In attesa che il garante rediga gli elenchi di soggetti tenuti alla valutazione d'impatto sulla protezione dei dati (necessaria proprio se il titolare svolge trattamenti di dati su larga scala), ai sensi dell'art. 35 comma 4 del GDPR, CNGEI ha valutato di non doversi dotare di un DPO.

SEZIONI TERRITORIALI QUALI RESPONSABILI DEL TRATTAMENTO

L'art. 28 del GDPR prevede effettivamente la figura del "Responsabile del Trattamento" inteso come una persona fisica o giuridica (es. società) che svolge, su incarico scritto del Titolare o sulla base di un contratto stipulato con il Titolare, un trattamento dei dati "per conto" del Titolare.
Le sezioni territoriali, che giuridicamente sono associazioni autonome, nella gestione dei dati degli iscritti, rientrano perfettamente nella definizione dell'articolo 28, laddove il CNGEI come associazione, ha il ruolo di Titolare del trattamento.
In considerazione di ciò sono le sezioni sono state inquadrate come Responsabili Esterne del trattamento ed è stato predisposto l'opportuno Atto di Nomina.

SOGGETTI AUTORIZZATI AI TRATTAMENTI

La figura dell'Incaricato del Trattamento (precedentemente prevista dall'art. 30 del Codice Privacy) non è espressamente prevista dal GDPR, che l'ha sostituita con il concetto di persona autorizzata al trattamento sotto l'autorità diretta del Titolare.
Al di là dell'innovazione terminologica, il concetto di fondo resta lo stesso ed il CNGEI ha individuato e autorizzato all'interno della propria organizzazione tutti i soggetti che all'interno e per conto dell'Associazione trattano dati personali (Presidente, Capo Scout, Consiglieri, Commissari e Responsabili Nazionali, dipendenti, ecc.), anche tenendo conto delle seguenti considerazioni:

- 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;
- 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;

CNGEI consegna 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.
CNGEI redige e aggiorna periodicamente anche una "lista degli incaricati", puntualmente formati 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.
Compito delle sezioni è quello di procedere all'individuazione e designazione dei soggetti autorizzati che operano all'interno della propria organizzazione autonoma (Ad es. CdS , CoS , CENS, CU, VCU e/o altri ruoli di sezione che entrano in contatto con i dati personali dei soci).

MISURE DI SICUREZZA ADEGUATE

Il GDPR, agli art. 24 e 33, non prevede più che le misure di sicurezza siano definite dalla legge o da un documento tecnico, come avveniva con il codice privacy, 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".

il nuovo principio di accountability (responsabilizzazione) introdotto dal GDPR implica quindi:

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

CNGEI ha implementato il proprio sistema interno di adozione delle misure ritenute adeguate in conseguenza della considerazione relativa al fatto che qualsivoglia trattamento informatico di dati non possa ormai prescindere dall'adozione delle vecchie "misure minime", e cioè dalla predisposizione:

- di un sistema di AUTENTICAZIONE INFORMATICA, di AUTORIZZAZIONE e di PROTEZIONE del sistema informatico da virus e accessi indesiderati, al fine di "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"
- di 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)
Gli ulteriori strumenti e metodi, indicati all'art. 26 e 32 del GDPR nell'ambito del principio cd. della "privacy by default", hanno portato ad implementare 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;
- non siano resi accessibili dati personali a chi non ne ha titolo e comunque mai in numero indefinito, in modalità automatica;
- sono adottate procedure per verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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, sono state identificate le principali misure adeguate in caso di trattamento dei dati svolto senza strumenti elettronici.
CNGEI ha attinto alle precedenti previsioni del Codice Privacy, secondo cui vanno fornite istruzioni scritte agli incaricati/autorizzati per il controllo e la custodia degli atti e documenti contenenti dati personali
In sostanza l'associazione ha stabilito 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 le sedi, centrale e territoriali, atti o documenti riguardanti l'ente o gli iscritti e nel riporli in appositi armadi chiusi a chiave, soprattutto se si tratta di dati sensibili.
Sono anche stati individuati gli ambiti di trattamento dei dati consentiti agli incaricati/autorizzati al trattamento e il loro aggiornamento almeno annuale.
CNGEI ha stabilito per iscritto le persone, appartenenti a categorie omogenee (es. iscritti con ruoli organizzativi pro tempore, membri del consiglio, dipendenti e collaboratori) autorizzate a compiere le attività di trattamento dei dati, con specificazione dei limiti e modalità
La verifica e l'eventuale modifica di tali incarichi avviene almeno una volta l'anno. La verifica viene fatta per i casi in cui l'incaricato cessi di trattare dati (es. cessazione delle cariche o degli eventuali rapporti di lavoro ecc.) o venga modificato l'ambito del suo trattamento.
Viene assicurato l'accesso controllato agli archivi e documenti contenenti dati sensibili, verificando 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.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'articolo 30 del 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;

Il Registro rientra dunque tra quegli elementi "documentali" tramite i quali il Titolare dimostra l'adeguamento al GDPR 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.
L'art. 30 del GDPR stabilisce che non sono tenuti alla redazione e conservazione dei Registri 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".
CNGEI, pur non ritendendo di essere obbligatoriamente tra i soggetti che hanno l'obbligo della tenuta del Registro, in via cautelativa e in base alla circostanza per cui facilmente i trattamenti e le attività delle ODV coinvolgono diritti fondamentali o dati sensibili ha deciso di predisporre il proprio Registro dei trattamenti in qualità di Titolare.
Il Registro, che sarà sottoposto a periodici aggiornamenti (almeno annuali) ha forma scritta ed è conservato presso la sede centrale.
Analogo registro dovrà essere tenuto anche dalle Sezioni locali, quali responsabili al trattamento dei dati.

SANZIONI

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.
Le sanzioni amministrative previste dall'art. 83 del GDPR sostituiscono quelle previste dall'attuale Codice italiano.
In sintesi:

- è soggetta alla sanzione pecuniaria (multa) "fino a € 10.000.000,00" la violazione degli obblighi gravanti sul Titolare e sul Responsabile del trattamento previsti dagli articoli 8, 11, da 25 a 39, 42 e 43; la violazione degli obblighi stabiliti dall'organismo di certificazione a norma degli articoli 42 e 43; la violazione degli obblighi stabiliti dall'organismo di controllo a norma dell'articolo 41, paragrafo 4.
    - Si tratta ad esempio delle seguenti ipotesi: trattamento senza consenso dei dati del minore, mancata redazione dei registri del trattamento o mancata adozione delle misure adeguate, mancata notifica al garante o all'interessato del data breach, (oppure mancata

esecuzione della dspia o mancata designazione del dpo, quando necessarie).

- è soggetta alla sanzione pecuniaria (multa) "fino a € 20.000.000,00" ad esempio la violazione:
  - dei "principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9";
  - dei "diritti degli interessati a norma degli articoli da 12 a 22";
  - 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 sulla liceità, base giuridica e finalità dei trattamenti, sulla pertinenza ed esattezza dei dati, sul consenso al trattamento dei dati comuni e "particolari", sull'obbligo e contenuto dell'informativa e sugli altri diritti degli interessati (rettifica, oblio, limitazione, portabilità, opposizione).

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

In un impianto sanzionatorio così pesante occorre tenere presente la possibilità, non certa né probabile, che le sanzioni amministrative possano essere valutate di volta in volta nella loro quantificazione, prendendo spunto dal fatto che il GDPR indica specifici elementi che possono provocare, anche l'applicazione di una sanzione di basso importo (l'art. 83 non prevede un importo minimo della sanzione), tra cui:

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

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, nella quale il Garante può chiedere al titolare, al responsabile, all'interessato o a terzi di fornire informazioni o esibire documenti. L'irrogazione della sanzione è disciplinata dalla L. 689/81: il Garante, se ritiene si sia compiuto l'illecito, notifica la contestazione; entro 60 giorni chi la riceve può far pervenire sue difese e chiedere di essere sentito; se il Garante conferma la violazione emette una ordinanza ingiunzione di pagamento, che è impugnabile davanti al giudice del luogo in cui è stato commesso l'illecito entro 30 giorni dalla notifica dell'ordinanza .
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:

- l'associazione se l'illecito è compiuto dai suoi dipendenti;
- il proprietario della cosa che è servita a commettere l'infrazione (es. l'associazione quale proprietaria del computer);
- la persona che aveva la vigilanza su chi ha commesso l'illecito, salvo

non provi di non aver potuto impedire il fatto

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

Altro potere del Garante è quello, previsto dall'art. 143 del Codice e 58 del GDPR, di imporre il blocco o la sospensione del trattamento illecito, di prescrivere al titolare l'adozione di idonee misure per renderlo lecito.
L'applicazione delle sanzioni amministrative è solitamente condizionata dalla gravità del fatto.
L'associazione può anche essere colpita da responsabilità civile (patrimoniale, da fatto illecito).
L'art. 82 GDPR, infatti, prevede che chiunque subisca un danno materiale o immateriale causato dalla violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
Si tratta di un'ipotesi di responsabilità oggettiva (da "attività pericolosa"), in quanto:

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

Quindi se CNGEI violasse le norme del Regolamento causando un danno a terze persone, potrà esser chiamata in causa dal danneggiato davanti al giudice civile per ottenere il risarcimento del danno patrimoniale e/o morale e risponderà con i beni dell'associazione.
Sul piano penale, di competenza di ciascuno Stato membro, attualmente restano applicabili i reati previsti dal Codice Privacy "armonizzato" (D.Lgs. n. 101/2018) con pene che prevedono anche la reclusione da sei mesi e tre anni, a seconda dei casi, o ammende pecuniarie.
All'interno dell'associazione, la responsabilità penale colpisce chi ha la rappresentanza legale e sotto il profilo sostanziale, esercita il potere direttivo e ha preso le decisioni in materia di trattamento dei dati personali.