legalitax
STUDIO LEGALE E TRIBUTARIO

VADEMECUM

IN MATERIA DI *PRIVACY*

E RELATIVI ADEMPIMENTI

REALIZZATO PER ANCESCAO

(ASSOCIAZIONE NAZIONALE CENTRI SOCIALI, COMITATI ANZIANI E ORTI)

E PER ESSERE DIRAMATO

A TUTTI I CENTRI SOCI ANCESCAO

6 settembre 2018

SOMMARIO

1. INTRODUZIONE

Il 25 maggio 2018 è entrato in vigore in tutti i Paesi Europei il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (in seguito "**GDPR**"), adottato dal Parlamento Europeo e dal Consiglio il 27 aprile 2016.

Tutti coloro che trattano dati personali nell'ambito delle proprie finalità istituzionali (ovvero non per scopi meramente personali), vale a dire i "Titolari del trattamento", che agiscono direttamente o per il tramite dei c.d. "Responsabili del trattamento" o dei propri Incaricati al trattamento, hanno l'obbligo di uniformarsi alla nuova normativa, pena l'applicazione di pesanti ed inasprite sanzioni, soprattutto pecuniarie.

Il GDPR ha infatti una portata generale e si applica a qualunque trattamento di dati personali di persone fisiche (c.d. Interessati) che si trovano nel territorio dell'UE, anche se effettuato da soggetti (Titolare del trattamento o Responsabile del trattamento) non stabiliti nell'UE, quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi ai suddetti Interessati nell'UE oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo nell'UE (art. 3 GDPR).

In vista dell'entrata in vigore del GDPR il tema della *privacy*, ovvero della protezione e tutela dei dati personali, ha fatto irruzione in ogni aspetto della vita quotidiana e dei rapporti lavorativi con un'intensità sorprendente. Gran parte di noi ha ricevuto numerose *email* che chiedevano di prestare/rinnovare il consenso al trattamento dei propri dati personali, ha firmato informative *privacy* aggiornate alle disposizioni del GDPR, qualcuno si è forse disiscritto da *newsletter*, ha aggiornato le impostazioni *privacy* dei propri profili sui *social*, ecc…

Il GDPR ha sicuramente cambiato la prospettiva con la quale il tema della *privacy* va affrontato, per le numerose disposizioni introdotte e gli altrettanti numerosi specifici adempimenti previsti.

Ad esempio, il GDPR non indica più le "misure minime" da attuare, ma impone la responsabilità (*accountability*) di definire le misure più adeguate tra tutte quelle possibili, e di garantire poi la conformità (*compliance*) dei trattamenti eseguiti.

Ciò implica la libertà del Titolare del trattamento nell'approntare le misure adeguate alla protezione dei dati personali, senza basarsi solamente su modelli precompilati o documentazione *standard*: oltre a prevedere delle misure di base (in applicazione del principio denominato "*privacy by default*"), ciascun Titolare del trattamento dovrà adottare delle procedure modellate sulle necessità e caratteristiche specifiche del trattamento svolto all'interno della propria realtà (c.d. "*privacy by design*"). Tutto ciò con lo scopo precipuo di assicurare la protezione delle persone fisiche (i soggetti Interessati) nel trattamento dei propri dati personali, specialmente di quelli un tempo definiti "sensibili" ed ora "appartenenti a categorie particolari".

Protezione equivale a *privacy*, ovvero al rispetto etico dovuto agli altri, ed è un'esigenza che opera in ogni campo, per il solo fatto che esista un rapporto tra soggetti, a maggior ragione quando per l'utilizzazione dei dati è necessario un espresso consenso. È un territorio vastissimo e senza limiti

che impone doveri di vigilanza, controllo, informazione e protezione nei confronti di una serie innumerevole di soggetti, con i quali si costituisce un rapporto (ad esempio i dipendenti, gli iscritti alle associazioni, i fornitori, i consulenti e così via).

Nell'ambito di questa enorme platea, devono essere posti in essere una serie di adempimenti e deve essere assicurato sempre e comunque il rispetto dei principi che regolano la materia: la liceità e la correttezza, la trasparenza, la buona amministrazione, l'accuratezza, l'integrità e la confidenzialità, insieme con altri princìpi particolari quali il principio di finalità, di necessità e minimizzazione e di limitazione all'archiviazione.

Vi è poi l'Interessato, ovvero la persona fisica i cui dati personali vengono trattati, rispetto alla quale il GDPR estende e rafforza i diritti: il diritto di accesso, il diritto alla rettifica, all'oblio, alla limitazione del trattamento, alla opposizione, alla portabilità dei dati e a ricevere le informazioni urgenti e immediate, e le notifiche relative, in caso di violazione dei suoi diritti, anche da parte di terzi.

Di *privacy* se ne è già parlato tanto, ma se ne continuerà a parlare ampiamente anche nei prossimi mesi, dal momento che il quadro normativo e regolamentare italiano è ancora in divenire.

Come tutti sappiamo, esisteva già il codice della *privacy* (D. Lgs. 196/2003 – in seguito il "**Codice**"), all'avanguardia nello scenario europeo e vanto della legislazione nostrana, al quale eravamo tutti abituati a fare riferimento.

In un primo momento, sembrava che esso dovesse essere integralmente abrogato dal legislatore italiano per lasciare che ogni aspetto fosse regolamentato dal GDPR. Tale soluzione, sicuramente più semplice, rischiava di creare numerose lacune non colmate dal GDPR. Si è dunque deciso di procedere nella più complessa strada dell'armonizzazione e coordinamento del Codice al GDPR.

Dopo un lungo e travagliato iter parlamentare, ricevute le osservazioni espresse dal Garante della Protezione dei Dati Personali (di seguito il "**Garante**"), in data 8 agosto 2018 il Consiglio dei Ministri ha finalmente approvato il Decreto Legislativo con il quale, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), ha introdotto le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR (di seguito il "**Decreto Attuativo**").

Il Decreto Attuativo è stato pubblicato in Gazzetta Ufficiale il 4 settembre 2018 (due giorni indietro rispetto alla redazione del presente vademecum).

Dal comunicato stampa n. 14 pubblicato sul sito del Consiglio dei Ministri in data 8 agosto 2018 si apprende che "*dopo l'esame di una commissione appositamente costituita si è deciso, al fine di semplificare l'applicazione della norma, di agire novellando il Codice, nonostante il GDPR abbia di fatto cambiato la prospettiva dell'approccio alla tutela della privacy rispetto al Codice introducendo il principio dell'accountability. Si è scelto di garantire la continuità facendo salvi per un periodo transitorio i provvedimenti del Garante e le relative autorizzazioni, che saranno oggetto di successivo riesame, nonché i Codici deontologici vigenti. Essi restano fermi nell'attuale configurazione nelle materie di competenza degli Stati membri, mentre possono essere riassunti e modificati su iniziativa delle categorie interessate quali codici di settore. In considerazione delle*

esigenze di semplificazione delle micro, piccole e medie imprese, si è previsto che il Garante promuova modalità semplificate di adempimento degli obblighi del titolare del trattamento".

Occorrerà dunque ancora un po' di tempo per interpretare le modifiche apportate al Codice e comprendere come lo stesso è stato integrato per adattarlo alle disposizioni introdotte dal GDPR e, soprattutto, per prendere piena cognizione e dare completa attuazione al nuovo quadro normativo e regolamentare (che verrà ulteriormente integrato e dovrà essere interpretato anche alla luce delle indicazioni che verranno fornite dal Garante e anche dalle linee guida del Gruppo di Lavoro dei Garanti *Privacy* europei).

Ne consegue, inevitabilmente, che le indicazioni fornite nel presente *vademecum* sono suscettibili di possibili integrazioni/revisioni alla luce del quadro normativo e regolamentare che si verrà a delineare nei prossimi mesi.

Ciononostante, si è ritenuto opportuno redigere e diramare fin da ora il presente *vademecum*, per consentire ad Ancescao e a tutti i Centri Soci Ancescao di familiarizzare e rafforzare la propria cognizione della materia e adeguarsi prontamente, ponendo in essere una serie di adempimenti da essa previsti, prima che - cessato il c.d. "periodo di moratoria" – aumenti l'attività ispettiva e di controllo demandata al Garante e relativa all'applicazione e rispetto del GDPR da parte di tutte le realtà che trattano dati personali nell'ambito della propria attività istituzionale.

Con il Decreto Attuativo il Governo ha, infatti, previsto un periodo di moratoria di otto mesi nel corso del quale i controlli del Garante (che si svolgeranno con l'ausilio della Guardia di Finanza) saranno attenuati, al fine di tenere conto della "*fase di prima applicazione delle disposizioni sanzionatorie*".

Risulta dunque quanto mai opportuno leggere con attenzione il presente *vademecum* che, senza pretese di esaustività e completezza, data la complessità e ampiezza della materia, vuole essere di primo aiuto e di supporto pratico ad Ancescao e a tutti i relativi Centri soci, al fine di acquisire consapevolezza della tutela da garantire agli aventi diritto ma anche delle sanzioni, inasprite dal GDPR, al fine di effettuare una consapevole valutazione del rischio e attuare gli adempimenti applicabili e necessari per rendersi *compliant*.

2. ALCUNE DEFINIZIONI

Cookies	*files* di testo registrati su supporto informatico, che permettono di registrare alcuni parametri e dati comunicati al sistema informatico, attraverso il *browser* utilizzato dall'utente del sito. Tali strumenti consentono pertanto un'analisi delle abitudini dell'utente nell'utilizzo del sito, per differenti finalità: esecuzione di autenticazioni informatiche, monitoraggio di sessioni, memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al server, memorizzazione delle preferenze, etc…
Dato personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile (Interessato).
Interessato	persona fisica identificata o identificabile. E' identificabile la persona fisica che può essere identificata, direttamente o indirettamente, mediante il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Iscritti	ogni persona fisica che si iscrive a un Centro Socio Ancescao e in tal modo diviene un tesserato Ancescao
larga scala	il numero degli interessati coinvolti, il volume dei dati trattati, la durata delle attività di trattamento o l'estensione geografica del trattamento rende impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità (es: trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività; trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico; trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo a clienti di una catena internazionale; trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o una banca nell'ambito delle ordinarie attività; trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale; trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici).
Particolari categorie di dati	dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, politiche o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Si tratta dei dati definiti "sensibili" dal Codice.
Trattamento	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, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

3. PRINCIPI GENERALI

Liceità e correttezza

Ogni Trattamento di Dati personali deve essere svolto in maniera lecita e corretta, **informando** l'Interessato circa la raccolta, l'utilizzo ed altri eventuali successivi trattamenti dei dati forniti.
Per essere lecito, il Trattamento di Dati personali deve fondarsi sul **consenso** dell'interessato o su **altra base giuridica** prevista dal GDPR o dal Codice.

Finalità e pertinenza

Tale principio prevede che vi sia una corrispondenza tra quanto dichiarato dal Titolare del Trattamento e quanto effettivamente accade nel Trattamento dei dati. Pertanto, i Dati personali raccolti e trattati devono essere adeguati, pertinenti e, soprattutto, limitati a quanto necessario per le finalità del Trattamento dichiarato.
L'esplicitazione delle finalità di Trattamento deve essere antecedente all'acquisizione del consenso e all'inizio delle attività di Trattamento poiché solo in tal modo è possibile garantire che il consenso dell'Interessato sia effettivamente informato.

Trasparenza

Per essere trasparente il Trattamento dovrà essere effettuato secondo modalità predefinite e previamente rese note all'Interessato, che sarà quindi pienamente consapevole non solo della tipologia di dati raccolti, ma anche delle modalità con cui tali dati sono stati raccolti e verranno trattati.
La trasparenza non riguarda solo il contenuto delle informazioni, ma anche le modalità con cui tali informazioni sono fornite all'interessato.

Necessità e minimizzazione

Tale principio prevede che non vi sia alcuna eccedenza nei trattamenti di dati. Pertanto, il Trattamento deve essere necessariamente vincolato alle finalità dichiarate dal Titolare nell'informativa.
Nell'effettuare il Trattamento con strumenti informativi, il Titolare dovrà preferire l'utilizzo di dati anonimi rispetto al Trattamento di Dati personali (che dovranno invece essere oggetto del Trattamento solo qualora vi sia la necessità d'identificare l'Interessato). In applicazione di tale principio i programmi informatici dovranno essere configurati per preferire l'utilizzo di dati anonimi laddove possibile.

Accuratezza

Il Titolare del Trattamento deve verificare che i dati raccolti siano corretti, veritieri e completi; deve trattare dati esatti e deve organizzare la propria struttura al fine di garantire il controllo sulla veridicità.

Il Titolare ha quindi l'obbligo di garantire un elevato *standard* di qualità nel Trattamento dei dati, dal momento che il Trattamento di Dati personali inesatti o incompleti potrebbe determinare una falsa rappresentazione dell'Interessato e comportare conseguenze indesiderate.

Integrità e confidenzialità

Il Titolare del Trattamento deve adottare tutte le misure ragionevoli affinché Dati personali inesatti siano rettificati o cancellati.
I Dati personali devono essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, e impedirne l'accesso o l'utilizzo non autorizzato, ad esempio mediante l'adozione di adeguate misure di sicurezza (protezione con password di accesso, pseudonimizzazione e cifratura).

Limitazione all'archiviazione

La conservazione dei dati, che costituisce una modalità di Trattamento, deve essere effettuata solo per il tempo strettamente necessario agli scopi stabiliti nelle finalità del Trattamento.
Tuttavia, occorre contemperare tale diritto con l'esigenza del Titolare di adempiere ad obblighi di legge che impongono determinati obbligo di conservazione dei dati (ad esempio obbligo di conservazione delle scritture contabili).

4. LE FIGURE RILEVANTI

4.1 Il Titolare del trattamento

E' 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 (art. 4, punto 7, GDPR).

Il Titolare del trattamento ha la responsabilità in merito alla valutazione del rischio e all'organizzazione degli strumenti e delle procedure idonei a tutelare i diritti degli Interessati; ha l'onere di provare di aver adottato misure organizzative e tecniche coerenti con le prescrizioni del GDPR, anche con riferimento alla periodica verifica dell'effettivo funzionamento delle misure di sicurezza adottate.

- Sulla base delle informazioni raccolte in sede di intervista dei rappresentanti Ancescao:

- per i Dati personali raccolti da Ancescao (si pensi ai dati personali dei dipendenti, fornitori e consulenti di Ancescao, come pure agli eventuali dati personali dei rappresentanti dei soci Ancescao, ovvero dei Centri Soci, sotto forma di Associazioni di Promozione Sociale, Organizzazioni di Volontariato o altre organizzazione riconosciuta dall'ordinamento del Terzo Settore e che si associano ad Ancescao), il Titolare del Trattamento è Ancescao, che agisce nella persona del proprio rappresentante (Presidente);

- per i Dati personali raccolti dai singoli Centri Soci Ancescao (si pensi ai Dati personali degli Iscritti) Titolare del Trattamento è il singolo Centro Socio Ancescao (vale a dire il singolo Centro Sociale, sotto forma di Associazione di Promozione Sociale, Organizzazione di Volontariato o altra organizzazione riconosciuta dall'ordinamento del Terzo Settore) che aderisce e si associa ad Ancescao e che a sua volta agisce nella persona del proprio rappresentante (Presidente).

- Ancescao, al momento, non riceve i Dati personali degli Iscritti e non influisce in alcun modo sulle modalità o finalità di Trattamento di tali dati. Pertanto i singoli Centri soci Ancescao sono autonomi Titolari del Trattamento in relazione a tali dati. Qualora in futuro, anche per effetto di possibili modifiche normative o regolamentari nel Terzo Settore, gli obblighi a carico di Ancescao dovessero mutare e quest'ultima dovesse essere tenuta a raccogliere e trattare i Dati personali degli Iscritti, si segnala che il GDPR prevede anche la figura de:

4.2 I Contitolari del Trattamento

"*Allorché due o più Titolari del Trattamento determinano congiuntamente le finalità e i mezzi del Trattamento, essi sono Contitolari del Trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal*" GDPR "*con particolare riguardo all'esercizio dei diritti dell'Interessato, e le rispettive funzioni di comunicazione delle informazioni*" da fornire in sede di informativa (art. 26 e Considerando 79 GDPR).

L'accordo interno riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli Interessati. Il contenuto essenziale dell'accordo interno è messo a disposizione dell'Interessato che, indipendentemente dalle disposizioni dell'accordo interno, potrà esercitare i propri diritti nei confronti di e contro ciascun Titolare del Trattamento.

Ciascun Titolare del Trattamento dovrà poi espletare gli adempimenti richiesti, in rapporto anche alla natura dei dati trattati, con riferimento alla propria gestione.

4.3 Il Responsabile del Trattamento

E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati personali per conto del titolare del Trattamento (art. 4, punto 8, GDPR).

È la persona incaricata (con atto di nomina a Responsabile del Trattamento) dal Titolare del Trattamento a:

- trattare i dati,
- supervisionare il Trattamento dei dati da parte dei soggetti autorizzati;
- implementare le misure di sicurezza;
- tenere il registro delle attività di Trattamento svolte, laddove obbligatorio o istituito su base volontaria (si veda il seguente paragrafo 5.2.6);
- eventualmente (se non fatto dal Titolare) designare il DPO, laddove obbligatorio o nominato su base volontaria (si veda il seguente paragrafo 4.5).

➢ Le articolazioni territoriali di un Ente nazionale possono ricevere il conferimento del ruolo di Responsabili del Trattamento dei dati inerenti tesseramento/affiliazione.

4.4 L'Amministratore di sistema

E' un particolare Responsabile del Trattamento la cui nomina è obbligatoria quando si trattano dati sensibili a mezzo di strumenti informatici, a cui vanno affidati i seguenti compiti:

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

4.5 Il Responsabile della protezione dati ("RPD") anche detto *Data Protection Officer* ("DPO")

E' una nuova figura introdotta dal GDPR. La relativa nomina è obbligatoria solo nei seguenti casi:

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

➢ <u>Anche laddove non obbligatorio per legge, il Titolare del Trattamento e il Responsabile del Trattamento possono nominare il DPO su base volontaria.</u>

L'incarico di DPO può essere ricoperto alternativamente da:

a) un dipendente/collaboratore dell'associazione, che non sia in conflitto di interessi,
b) un soggetto esterno

a condizione che possieda un'approfondita conoscenza della normativa e delle prassi in materia di *privacy* (persona che presenti "*garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR, anche per la sicurezza del Trattamento*" - Considerando 81 GDPR).

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

Qualora non sia nominato il DPO, tali compiti dovranno essere assolti dal Titolare o dal Responsabile del Trattamento.

I compiti del DPO sono:

a) informare e fornire consulenza al Titolare del Trattamento o al Responsabile del Trattamento nonché ai collaboratori che eseguono il Trattamento in merito agli obblighi introdotti dalla normativa;
b) sorvegliare l'osservanza della normativa in materia;
c) curare la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
d) fornire, se richiesto e laddove previsto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
e) cooperare con l'autorità di controllo (Garante).

4.6 L'Incaricato al Trattamento dei dati

Il Titolare del Trattamento o il Responsabile del Trattamento dei dati – con l'eventuale supporto del DPO – dovrà procedere a:

- nominare e autorizzare per iscritto gli Incaricati al Trattamento (dipendenti/collaboratori che trattano i dati e accedono a determinate banche-dati) fornendo specifiche istruzioni sulle finalità e modalità del Trattamento delle specifiche categorie di dati trattati dall'Incaricato;
- verificare che gli Incaricati al Trattamento dei dati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale alla riservatezza (art. 28 GDPR);
- sensibilizzare e formare gli Incaricati al Trattamento al tema della *privacy*, sia con riferimento ai vincoli normativi che con riferimento alle procedure/strumenti adottati internamente per garantire il rispetto del GDPR.

5. GLI ADEMPIMENTI

5.1 Alcune domande ricorrenti:

- Con l'entrata in vigore del GDPR devo rifare tutto? Gli adempimenti *privacy* posti in essere per il passato non valgono più?

NO, se abbiamo espletato gli adempimenti già previsti dal Codice

- Devo chiedere di nuovo il consenso al Trattamento dei dati?

NO, se posso provare di averlo già acquisito, se invece non ho conservato la documentazione cogliamo l'occasione della riforma per richiederlo

SI, se non posso provare di averlo acquisito o quando le finalità del Trattamento sono cambiate rispetto a quelle originariamente indicate.

- Devo rifare l'informativa?

SI, sarà necessario aggiornarla con alcuni elementi

- Devo adottare nuove misure di sicurezza?

Dipende dal rischio nel Trattamento dei dati. Prima è necessario fare un percorso di informazione/formazione ed analisi del contesto/valutazione del rischio

- Devo nominare il Responsabile della protezione dei dati (DPO)?

Non è necessario sempre, potrebbe essere utile anche quando non obbligatorio

5.2 Quali sono gli adempimenti *privacy* introdotti dal GDPR e/o già esistenti?

5.2.1. Valutazione del rischio e analisi organizzativa caso per caso (novità)

5.2.2. Adozione di misure di sicurezza idonee (già previsto, da integrare eventualmente)

5.2.3. Informativa (già prevista, da integrare)

5.2.4. Acquisizione del consenso (già prevista)

5.2.5. Conferimento degli incarichi (già previsto, da integrare eventualmente con la nomina del DPO)

5.2.6. Istituzione e aggiornamento del Registro del Trattamento dei dati (novità)

5.2.7. Formazione degli operatori (già previsto ma rafforzato)

5.2.8. Notifica della violazione della *privacy* – c.d. *data breach* (novità)

5.2.1 Valutazione del rischio e analisi organizzativa caso per caso (novità)

Si tratta della c.d. Valutazione d'impatto sulla protezione dei dati (c.d. *Data Protection Impact Assessment* – "**DPIA**")

L'art. 35 del GDPR prescrive l'onere, in capo al Titolare del Trattamento, di compiere in via preliminare al Trattamento una valutazione d'impatto sulla protezione dei dati "*quando un tipo di Trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del Trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

La DPIA è richiesta in modo particolare se il Titolare del Trattamento effettua:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un Trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il Trattamento, su larga scala, di categorie particolari di Dati personali o di dati relativi a condanne penali o a determinati reati; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

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

La DPIA serve per determinare, in particolare, "*l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il Trattamento dei Dati personali rispetta*" il GDPR (considerando 84 GDPR).

La DPIA contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del Trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del Trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei Dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

- Sulla base delle informazioni raccolte in sede di intervista dei rappresentanti Ancescao, tale adempimento non dovrebbe essere obbligatorio per Ancescao. Non si ha contezza

completa di tutti i trattamenti svolti da ogni singolo Centro Socio Ancescao pertanto la valutazione viene rimessa ad ogni singolo destinatario del presente *vademecum*.

- Ad ogni modo si segnala che, anche laddove non obbligatoria, la DPIA può essere effettuata su base volontaria, ed anzi, è considerata buona prassi e consente al Titolare del Trattamento di identificare e gestire al meglio potenziali rischi che non sarebbero stati altrimenti rilevati e prevenire possibili violazioni che altrimenti si sarebbero verificate. Essa costituisce quindi uno strumento utile per dimostrare, in caso di ispezione del Garante, il rispetto del GDPR, in ossequio al principio di *accountability* (responsabilizzazione).

5.2.2 Adozione di misure di sicurezza idonee (già previsto, da integrare eventualmente)

Diversamente da quanto previsto dal Codice (art. 33-36 e Allegato B contenente il *Disciplinare tecnico in materia di misure minime di sicurezza*) il GDPR non prevede misure di sicurezza valide in ogni caso. In base al principio di responsabilizzazione, il Titolare e il Responsabile del Trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento, come anche del rischio, devono effettuare una valutazione caso per caso e adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR).

Le misure di sicurezza possono consistere (considerando 78, 79 e art. 32 GDPR) in:

1) ridurre al minimo il Trattamento dei Dati personali;
2) garantire trasparenza per quanto riguarda le funzioni ed il Trattamento dei Dati personali;
3) ripartire in modo chiaro le responsabilità nel Trattamento;
4) adottare le misure tecnologiche adeguate ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento (es: la pseudonimizzazione e la cifratura dei Dati personali).

Si tratta di una lista esemplificativa e non esaustiva.

Una buona prassi organizzativa è considerata anche la redazione da parte del Titolare e l'adozione e rispetto – da parte di tutti i Responsabili e Incaricati, nonché di tutti i dipendenti - di un regolamento per l'utilizzo dei sistemi informatici e delle banche dati cartacee.

Secondo il Garante, le misure minime di sicurezza previste dal Codice possono costituire "*un nucleo centrale minimo per garantire la sicurezza dei dati*" ma il Titolare e il Responsabile del Trattamento dovranno effettuare, caso per caso, una valutazione delle misure tecniche e organizzative più idonee a garantire un livello di sicurezza adeguato al rischio. Non è nemmeno possibile ritenere sufficiente o necessaria l'adozione delle misure di sicurezza riportate all'interno dell'art. 32 del GDPR, perché occorrerà sempre una valutazione caso per caso.

5.2.3 Informativa (già prevista, da integrare)

L'obbligo di rendere all'Interessato l'informativa *privacy* prima di effettuare un Trattamento di Dati personali raccolti presso l'Interessato[1] - salvo casi particolari[2] - era già previsto dal Codice (art. 13).

Il GDPR ha rafforzato/ampliato i diritti degli Interessati e dunque si rende necessario aggiornare le informative già fornite agli Interessati.

- Sebbene non sia espressamente previsto l'obbligo di fornire un'informativa scritta, è assolutamente raccomandabile fornire per iscritto l'informativa per documentare l'assolvimento dell'adempimento (principio di *accountability*). Si consiglia anche di raccogliere la firma dell'Interessato per presa visione[3].

L´informativa deve avere forma concisa, trasparente, intelligibile per l´Interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice.

- E' consigliabile elaborare informative specifiche per ciascuna tipologia di Interessato (es. informativa dipendenti, informativa fornitori, informativa Iscritti, *privacy policy* per gli utenti del sito *internet*, ecc…).

NB: ogni volta che le finalità di Trattamento cambiano, il GDPR impone di informarne l´Interessato prima di procedere al Trattamento ulteriore.

Elementi dell'informativa:

○ le finalità e le modalità del Trattamento cui sono destinati i dati	già previsto dal Codice
○ la natura obbligatoria o facoltativa del conferimento dei dati	già previsto dal Codice
○ la base giuridica del Trattamento (es: si basa sul consenso espresso dall'Interessato)	novità GDPR
○ le conseguenze di un eventuale rifiuto di rispondere	già previsto dal Codice
○ i soggetti o le categorie di soggetti ai quali i Dati personali possono essere comunicati o che possono venirne a conoscenza (in qualità di responsabili o incaricati, se nominati in tal senso in quanto trattano dati per conto del Titolare o in qualità di autonomi titolari del Trattamento, se estranei all'originario Trattamento eseguito dal Titolare) e l'ambito di diffusione dei dati medesimi	già previsto dal Codice
○ ove applicabile, l'intenzione del Titolare del Trattamento di	novità GDPR

[1] Nel caso di dati personali non raccolti direttamente presso l´Interessato (art. 14 GDPR), l´informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all´Interessato).

[2] Art. 13, paragrafo 4 e art. 14, paragrafo 5 GDPR, art. 23, paragrafo 1, GDPR - spetta al Titolare, in caso di dati personali raccolti da fonti diverse dall´interessato, valutare se la prestazione dell´informativa agli interessati comporti uno sforzo sproporzionato– a differenza di quanto prevede l´art. 13, comma 5, lettera c) del Codice.

[3] E' preferibile il formato elettronico (soprattutto nel contesto di servizi online: art. 12, paragrafo 1, e considerando 58 GDPR), anche se sono ammessi "altri mezzi", quindi può essere fornita anche in modalità cartacea. Il GDPR ammette l´utilizzo di icone per presentare i contenuti dell´informativa in forma sintetica, ma solo "in combinazione" con l´informativa estesa (art. 12, paragrafo 7. GDPR) - tali icone dovranno essere identiche in tutta l´UE e saranno definite prossimamente dalla Commissione Europea.

trasferire Dati personali a un Paese terzo o a un'organizzazione internazionale e, se del caso, attraverso quali strumenti (attenzione alle *newsletter* inviate attraverso programmi di invio massivo a *mailing-lists*)	
○ i diritti dell'Interessato	già previsto dal Codice (art. 7) ma da aggiornare con i nuovi diritti previsti dal GDPR (art. 15 e ss.)
○ gli estremi identificativi del Titolare del Trattamento e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 Codice e del Responsabile del Trattamento.	già previsto dal Codice
○ i dati del Responsabile della protezione dei Dati personali (DPO) se nominato	novità GDPR
○ l'esistenza di un processo decisionale automatizzato, compresa la profilazione (attenzione Google Analytics) indicando anche la logica di tali processi decisionali e le conseguenze previste per l´Interessato	novità GDPR
○ il periodo di conservazione dei dati o i criteri utilizzati per determinare tale periodo	novità GDPR

- Per quanto riguarda **i diritti dell'Interessato**, l'informativa può elencarli analiticamente[4] o fare rinvio agli art. 15 e ss. del GDPR. In ogni caso è importante indicare che l'Interessato ha diritto di presentare reclamo al Garante qualora il Titolare non fornisca riscontro alle richieste dell'Interessato nei tempi previsti (1 mese dalla richiesta - estendibile fino a 3 mesi in casi di particolare complessità – entro il quale il Titolare deve comunque dare un

[4] L'articolo 7 del Codice e gli art. 15 e ss. del GDPR conferiscono all'Interessato il diritto di ottenere:
- la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
- l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del Titolare;
- l'aggiornamento, rettifica, integrazione, cancellazione, trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge (compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono raccolti o successivamente trattati);
- l'attestazione che tali operazioni sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'Interessato ha inoltre il diritto:
- di revocare in qualsiasi momento il consenso prestato al trattamento dei dati personali (senza pregiudizio della liceità del trattamento basata sul consenso prestato prima della revoca);
- di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- di opporsi, in tutto o in parte al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale;
- di proporre reclamo al Garante nei casi previsti dal GDPR;
- alla portabilità dei dati personali (diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti) nei limiti di cui all'art. 20 GDPR.

riscontro all´Interessato anche in caso di diniego) o la risposta fornita dal Titolare non fosse soddisfacente.

- Per quanto riguarda le finalità del Trattamento, occorre tenere sempre a mente il **principio di pertinenza** del Trattamento alle finalità per le quali i dati sono stati raccolti (come dichiarato in informativa). Alcuni esempi:

  L'Associazione deve garantire l'assoluta trasparenza gestionale e quindi l'accessibilità ai verbali e al bilancio, ma le modalità di Trattamento devono essere pertinenti. Quindi se in bacheca espongo il cartello in cui invito i soci a versare il contributo annuale entro una determinata data, pena l'esclusione (se lo statuto prevede la morosità come causa di esclusione e quindi sancisce il termine a partire dal quale si configura) in bacheca NON espongo il nome dei soci morosi!

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

- In caso di utilizzo di un **sito *internet***, occorrerà pubblicare sul sito un'informativa *privacy* (c.d. *privacy policy* del sito) nella quale informare gli utenti del sito sulle modalità di gestione del sito per quanto attiene la raccolta di Dati personali dagli utenti del sito. In essa occorrerà indicare tutti gli elementi dell'informativa sopra elencati e anche informare gli utenti sui ***cookies*** utilizzati nel sito e sulle relative conseguenze per l'utente:

- *cookie* tecnici: servono ad effettuare la navigazione o a fornire un servizio richiesto dall'utente. Senza il ricorso a tali *cookie*, alcune operazioni non potrebbero essere compiute o sarebbero più complesse e/o meno sicure. Per l'utilizzo e installazione dei *cookie*s tecnici non è richiesto il consenso dell'utente.
- *cookie* di profilazione: sono utilizzati per tracciare la navigazione dell'utente e creare dei profili sui suoi gusti, abitudini, scelte, ecc. In questo modo possono essere trasmessi al dispositivo dell'utente messaggi pubblicitari in linea con le sue preferenze già manifestate nella precedente navigazione *online*. Per l'utilizzo e installazione dei *cookie* di profilazione è richiesto il consenso dell'utente. Nel caso in cui l'utente non desideri che il suo dispositivo riceva e memorizzi i *cookie* di profilazione, potrà modificare le impostazioni di sicurezza del suo *broswer* (cancellare e/o evitare l'installazione dei *cookie* sul dispositivo utilizzato); tuttavia disattivando l'utilizzo dei *cookie* di profilazione l'utente non potrà usufruire appieno di alcune funzioni del sito.
- *cookie* di terzi: particolare tipologia di *cookie* di profilazione che vengono inviati al dispositivo dell'utente da un dominio o da una pagina *web* non gestita direttamente dal Titolare, ma da un altro soggetto che analizza i dati ottenuti per raccogliere informazioni sull'uso del sito. E' bene elencare in informativa chi sono tali terze parti.

  È quindi necessario acquisire informazioni da chi gestisce il sito con particolare riferimento ai *cookies* o altri strumenti di profilazione che possono essere utilizzati (direttamente o indirettamente) perché occorrerà indicarlo in informativa. Ad esempio effettuano la

profilazione *Google Analytics, Youtube, Facebook*. Se vengono utilizzati attraverso il sito, è necessario specificare nell'informativa che il Trattamento dei dati prevede la profilazione e rinviare alla *privacy policy* del soggetto che realizza la profilazione.

- In caso di presenza sul sito di ***link* a siti terzi**, si consiglia di specificare in sede di *privacy policy* che il Titolare non ha alcuna responsabilità sui contenuti del sito terzo e di rinviare alla relativa *privacy policy*.

- Sia in caso di utilizzo di un sito *internet*, che di invio di ***newsletter*** mediante sistemi di invio automatizzato a liste di destinatari (c.d. *mailing-list*) che di utilizzo di pagine sui *social* (es. pagina *Facebook* di Ancescao o di Centri soci Ancescao) è anche necessario acquisire informazioni da chi gestisce il sito/*provider* del servizio di invio della *newsletter*/*social* con particolare riferimento ai luoghi ove vengono trasmessi i Dati personali raccolti (in particolare se l'utilizzo comporta trasferimento in Paesi extra Europei) perché tale informazione andrà indicata in informativa, dettagliando anche le cautele adottate nel caso di trasferimento dei dati extra UE verso Paesi che assicurino un livello inferiore di protezione dei dati.

  Es: i Centri soci Ancescao che forniscono un servizio di ***newsletter*** ai propri soci potrebbero trasferire extra UE in maniera inconsapevole i Dati personali degli Iscritti, semplicemente utilizzando strumenti per l'invio di *newsletter* gestiti da società extra europee (es: MailChimp che ha sede negli USA). Tale aspetto va indicato in informativa e occorre fare rinvio all'informativa *privacy* del *provider* del servizio di *newsletter*. Per quanto riguarda MailChimp, tale società aderisce al c.d. Scudo *Privacy* (accordo bilaterale UE – USA che consiste in una decisione di adeguatezza dei trattamenti effettuati dalle imprese aderenti) e agisce quale contitolare del Trattamento.

- In caso di apertura di una **pagina *Facebook***:

  - si stipula un contratto con *Facebook* che prevede l'adesione alle condizioni generali *Facebook* di utilizzo della pagina *Facebook*, inclusa la politica ad essa relativa in materia di *cookie*;
  - *Facebook* posiziona sul *computer/smartphone* degli utenti che visitano la pagina *Facebook* (a prescindere dalla circostanza che abbiano un proprio profilo *Facebook* o meno), *cookie* per memorizzare informazioni nei *browser web* che, se non eliminati, restano attivi per due anni;
  - *Facebook* riceve, registra ed elabora le informazioni memorizzate nei *cookie* così come possono farlo i *partner* commerciali di *Facebook*;
  - l'amministratore di una pagina *Facebook* contribuisce al Trattamento dei dati e può, tramite filtri messi a disposizione da *Facebook*, definire i criteri a partire dai quali elaborare statistiche sulle navigazioni nella pagina *Facebook* (geolocalizzazione, età, sesso, situazione sentimentale e professionale, informazioni sugli interessi, le categorie di prodotti o di servizi di maggiore interesse degli utenti) e designare perfino le categorie di persone i cui Dati personali saranno oggetto di utilizzo da parte di *Facebook*;
  - in caso di apertura di una pagina *Facebook*, si diventa Responsabili del Trattamento effettuato da *Facebook* (Corte di Giustizia UE, sentenza 5/6/2018, causa C-210/16).

  In informativa occorre pertanto informare gli utenti che *Facebook* - attraverso *cookie* attivati sul disco rigido – tratta i relativi dati per realizzare statistiche sugli utenti destinate

all'amministratore della pagina *Facebook* e permettere a *Facebook* di diffondere pubblicità mirate.

5.2.4 Acquisizione del consenso (già prevista)

Al di fuori dei casi nei quali esiste una differente base giuridica che legittima il Trattamento dei dati[5] - e dunque si può procedere al Trattamento senza previamente raccogliere il consenso dell'Interessato - si rende necessario raccogliere e documentare l'acquisizione del consenso.

Il consenso può essere espresso verbalmente per i Dati personali "comuni" (non appartenenti a categorie particolari – sensibili per i quali è invece obbligatoria l'acquisizione per iscritto) ma è sempre e comunque preferibile che sia manifestato e acquisito per iscritto (principio di *accountabiliy*).

Deve essere un consenso espresso (non vale il principio del silenzio-assenso) e va prestato con specifico riferimento alle varie tipologie di Trattamento che il Titolare intende effettuare e che richiedono la prestazione del consenso.

È possibile acquisirlo attraverso moduli, ivi inclusi quelli *on-line*, ma non possono essere proposte caselle pre-spuntate (deve essere assicura la libertà di scelta e la facoltà di negare il consenso anche solo con riferimento a certi trattamenti).

Per i minori il Decreto Attuativo ha fissato in 14 anni il limite di età al di sopra della quale la prestazione del consenso da parte dell'Interessato sarà ritenuta valida ed efficace (al di sotto della quale è necessario che il consenso sia prestato dai genitori o chi ne fa le veci).

- Nel caso in cui il Trattamento dei dati assolva a più funzioni (per esempio l'associazione acquisisce i dati degli Iscritti per la gestione del rapporto associativo ma potrebbe trattare i medesimi dati anche per trasmettere comunicazioni commerciali, ad es. ***newsletter* o altre iniziative promozionali**) è necessario che il consenso sia espresso in maniera specifica per ogni singola finalità di Trattamento che richiede la prestazione del consenso.
  L'informativa dovrà informare gli Interessati che il conferimento dei Dati personali ai fini di ricezione della *newsletter*/iniziative promozionali è facoltativo e il mancato conferimento del consenso determina solo l'impossibilità di ricevere le *newsletter*/iniziativa promozionale (ma non implica l'impossibilità di ricevere gli altri servizi richiesti in fase di tesseramento e il rilascio della tessera associativa non può essere condizionato all'iscrizione al servizio di *newsletter* o, comunque, all'accettazione di altre iniziative promozionali).

[5] Art. 6 GDPR:
- esecuzione di un contratto di cui l'Interessato è parte;
- adempimento di un obbligo di legge;
- salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

Non si possono quindi utilizzare i dati degli Iscritti, raccolti in fase di tesseramento, per inviare *newsletter* sulle iniziative dell'associazione o altre iniziative promozionali se non previa specifica raccolta di consenso da parte dell'Iscritto a ricevere le *newsletter*/iniziative promozionali. Qualora l'associazione non abbia operato in tal senso in passato, sarà necessario fornire all'Iscritto un'informativa aggiornata e raccogliere il consenso specifico alla ricezione di *newsletter*/iniziative promozionali.

- Ogni singola *newsletter*/email inviata deve consentire ai destinatari di disiscriversi in ogni momento dal servizio (ad es. cliccando su un link alla funzione "disiscriviti") e i relativi Dati personali necessari all'invio della *newsletter*/email devono essere trattati solo per il periodo strettamente necessario (principio della minimizzazione dei trattamenti) in un modello di gestione c.d. "*opt-out*" (ovvero fino a quando l'Interessato eserciterà il diritto di disiscrizione dal servizio). Inoltre, come appreso in fase di intervista dei rappresentanti Ancescao, gli Iscritti che intendono beneficiare dei servizi Ancescao devono mantenere la propria associazione al Centro (socio di Ancescao) di appartenenza pagando la relativa quota associativa. In caso di cessazione di tale rapporto associativo, si consiglia anche di togliere il relativo soggetto dalle *mailing-list* di invio automatizzato delle *newsletter*.

5.2.5 Conferimento degli incarichi (già previsto, da integrare eventualmente con la nomina del DPO)

Già in vigenza del Codice (art. 29), era prevista la facoltà per il Titolare del Trattamento di designare uno o più **Responsabili del Trattamento** (individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza) con indicazione specifica per iscritto dei compiti affidati.

Il Responsabile del Trattamento tratta dati per conto del Titolare, attenendosi alle indicazioni ricevute dal Titolare.

Possono essere nominati **Responsabili del Trattamento interni all'ente o esterni** (ad es. laddove certi trattamenti vengano affidati a terzi, es. gestione del personale affidata a un consulente del lavoro/studio paghe; elaborazione del bilancio affidato a uno studio di commercialisti) occorrerà nominare per iscritto il consulente (studio paghe, commercialista, ecc…) Responsabile del Trattamento.

Si tratta di una facoltà in caso di affidamento di certi trattamenti a terzi, in quanto, in caso contrario (ovvero laddove il Titolare non si avvalga di terzi nel Trattamento di dati) i compiti e le responsabilità permarranno in capo al Titolare del Trattamento.

In ogni caso il Titolare ha la responsabilità sulla scelta della figura del Responsabile (*culpa in eligedo*) e deve vigilare sul rispetto delle istruzioni impartite (*culpa in vigilando*).

Tra i Responsabili del Trattamento vi è anche, laddove applicabile, la figura dell'**Amministratore di Sistema** (si veda il precedente paragrafo 4.4).

L'art. 30 Codice prevede anche che le operazioni di Trattamento possono essere effettuate solo da **Incaricati** che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle

istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l´ambito del Trattamento consentito.

Tali principi si ritrovano anche nel GDPR (art. 28: qualora un Trattamento debba essere effettuato per conto del Titolare del Trattamento, quest'ultimo ricorre unicamente a Responsabili del Trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'Interessato; art. 29: il Responsabile del Trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del Trattamento, che abbia accesso a Dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del Trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri).

Il Responsabile del Trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del Trattamento. Tutti i trattamenti sono disciplinati da un contratto che vincoli il Responsabile del Trattamento al Titolare del Trattamento e che disciplini i compiti, la durata del Trattamento, la natura e la finalità del Trattamento, il tipo di Dati personali e le categorie di Interessati, gli obblighi e i diritti del Titolare del Trattamento.

La novità introdotta dal GDPR in tema di conferimento di incarichi è la nomina, laddove obbligatoria o effettuata su base volontaria, del **DPO** (si veda il precedente paragrafo 4.5).

- **NB: tutte le nomine devono essere effettuate per iscritto e si consiglia sempre di raccogliere la firma per accettazione da parte del Responsabile – Incaricato – DPO (principio di *accountability*).**

5.2.6 Istituzione e a aggiornamento del Registro del Trattamento dei dati (novità)

E' un nuovo adempimento previsto dall'art. 30 GDPR, non obbligatorio per quelle imprese o organizzazioni che occupano meno di 250 dipendenti, a meno che

- il Trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'Interessato, o
- il Trattamento non sia occasionale, o
- il Trattamento includa il Trattamento di "categorie particolari di dati" o dati giudiziari relativi a condanne penali o a determinati reati.

E' un adempimento simile al Documento programmatico sulla sicurezza (DPS) previsto dal Codice e ora abrogato (che doveva essere redatto da quanti trattavano dati sensibili attraverso il *computer*).

Tra i contenuti del Registro del Trattamento dei dati si segnalano le seguenti informazioni:

- chi è e come si può contattare il Titolare/Contitolare/DPO (se nominato);
- finalità di Trattamento dei dati;
- tipologie di dati trattati e di trattamenti effettuati;
- basi giuridiche su cui si fonda il Trattamento e casi in cui è previsto il consenso degli Interessati (da dove risulta la prestazione del consenso);
- diverse categorie di Interessati;

- a chi possono essere comunicati i dati e se possono essere comunicati anche ad organizzazioni internazionali o ad organizzazioni con sede fuori dall'Europa e relative garanzie assicurate;
- denominazione Responsabili esterni (se nominati);
- modalità di conservazione dei dati;
- dopo quanto tempo o in che casi si procedere alla cancellazione dei dati;
- quali sono i rischi nel Trattamento dei dati e quali sono le misure di sicurezza tecniche e organizzative adottate;
- etc…

➢ Sulla base delle informazioni raccolte in sede di intervista dei rappresentanti Ancescao, tale adempimento non dovrebbe essere obbligatorio per Ancescao. Non si ha contezza completa di tutti i trattamenti svolti da ogni singolo Centro Socio Ancescao pertanto la valutazione viene rimessa ad ogni singolo destinatario del presente *vademecum*.

➢ Ad ogni modo si segnala che, anche laddove non obbligatorio, il Registro può essere istituito su base volontaria, ed anzi, l'istituzione e tenuta del Registro è considerata buona prassi ed è certamente un elemento utile, se non indispensabile, per ogni Titolare del Trattamento per dimostrare, in caso di ispezione del Garante, il rispetto del GDPR, in ossequio al principio di *accountability* (responsabilizzazione).

5.2.7 Formazione degli operatori (già previsto ma rafforzato)

L'art. 29 GDPR prevede che il Responsabile del Trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del Trattamento e che abbia accesso ai Dati personali (e dunque gli Incaricati del Trattamento) non può trattare tali dati se non è istruito in tal senso dal Titolare del Trattamento.

La centralità della formazione è confermata anche dall'art. 32, paragrafo 4, GDPR che prevede che il Titolare del Trattamento ed il Responsabile del Trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a Dati personali non tratti tali dati se non è istruito in tal senso dal titolare del Trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Occorre pertanto, anche per attuare il principio di *accountability*, che il Titolare effettui un'adeguata formazione ed istruzione del personale (Incaricati o responsabili del Trattamento) in materia di protezione dei dati. La formazione costituisce, infatti, una misura di sicurezza, un onere a carico del Titolare del Trattamento, un diritto e dovere per i dipendenti e i collaboratori.

Il Titolare del Trattamento dovrà quindi pianificare un piano di formazione e aggiornamento (dando priorità ai nuovi assunti e alle figure di maggior rilievo nel Trattamento dei dati), stanziare apposite risorse nei propri *budget*, pianificare *test* per verificare il livello di apprendimento e soluzioni alternative in caso di risultati negativi.

La formazione dovrebbe, alla luce dell'impianto del GDPR, presentare un taglio interdisciplinare (con sessioni sia informatiche sia giuridiche) e pragmatico e riguardare tutti i soggetti. Essa dovrebbe essere finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni.

Nel caso di mancata erogazione della formazione sono infatti applicabili le sanzioni elencate al seguente paragrafo 6.

L'adempimento degli obblighi formativi è inoltre spesso oggetto anche di accertamenti ispettivi da parte del Garante (che effettua tali ispezioni avvalendosi della Guardia di Finanza). Già in vigenza del Codice, infatti, il Garante, richiedeva, in sede di ispezioni, di acquisire il programma ed il piano di formazione in materia di *privacy*, i materiali erogati al personale, il *test* finale di valutazione e le istruzioni agli Incaricati al Trattamento.

5.2.8 Notifica della violazione della *privacy* – c.d. *data breach* (novità)

In caso di violazione dei Dati personali – a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà degli interessati – il Titolare del Trattamento è tenuto a notificare la violazione al Garante entro 72 ore dal momento in cui ne viene a conoscenza. In caso di ritardo nella notifica, deve specificare i motivi del ritardo.

La notifica deve almeno:

a) descrivere la natura della violazione dei Dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei Dati personali in questione;
b) comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei Dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del Trattamento per porre rimedio alla violazione dei Dati personali e anche, se del caso, per attenuarne i possibili effetti negativi (art. 33 GDPR).

Il Titolare del Trattamento deve documentare ogni violazione, le relative circostanze, conseguenze, i provvedimenti adottati (principio di *accountability*). Tale documentazione consente al Garante di verificare il rispetto del GDPR.

Quando la violazione dei Dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati, il Titolare del Trattamento comunica la violazione all'Interessato senza ingiustificato ritardo (art. 34 GDPR).

Alcuni esempi:

- Abbiamo perso la chiavetta all'interno della quale avevamo l'anagrafica dei soci?
- Abbiamo perso il faldone con i certificati medici degli atleti della nostra associazione sportiva?

Sono tutte violazione della privacy!

- Cosa dobbiamo fare?

1) dobbiamo documentare questa violazione (lo scriveremo in un verbale del Consiglio Direttivo o lo inseriremo nel Registro del Trattamento dei dati) ed indicare i provvedimenti adottati;

2) se l'associazione scopre una violazione dei Dati personali, qualora si ritenga che da tale violazione possano derivare rischi per i diritti e per le libertà degli Interessati, dovrà comunicarlo al Garante entro 72 ore e se il rischio per gli Interessati si ritiene elevato, è necessario informare anche loro della violazione.

6 LE SANZIONI

Il profilo sanzionatorio è uno degli aspetti di maggior rinnovamento portati dal GDPR.

Il Codice prevede sanzioni amministrative e penali per le ipotesi più gravi (quali il Trattamento illecito e la mancata previsione di misure di sicurezza, la falsità nelle dichiarazioni al Garante e l'inosservanza dei suoi provvedimenti).

Il GDPR prevede sanzioni amministrative pecuniarie:

(a) fino a 10 milioni di euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, ad esempio nei casi di

- violazione delle misure di sicurezza o non individuazione di tali misure
- mancata nomina del DPO nei casi in cui la nomina è obbligatoria per legge
- mancata istituzione e tenuta del Registro del Trattamento dei dati nei casi obbligatori per legge

(b) fino a 20 milioni di euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, ad esempio nei casi di

- mancata acquisizione del consenso
- mancata informativa all'Interessato sulle modalità di Trattamento dei suoi dati e sui suoi diritti

Il Garante dovrà provvedere affinché le sanzioni amministrative pecuniarie inflitte ai sensi del GDPR siano in ogni singolo caso effettive, proporzionate e dissuasive.

Gli Stati Membri potranno introdurre norme relative ad altre sanzioni per le violazioni del GDPR, in particolare per le violazioni non soggette alle sanzioni amministrative pecuniarie sopra indicate. Tali sanzioni dovranno essere effettive, proporzionate e dissuasive.