Per agevolare le associazioni nel processo di adeguamento alle principali novità introdotte dal nuovo Regolamento ho redatto una relazione che illustra la normativa del GDPR e individua gli adempimenti di cui sono onerati gli ETS (Enti del Terzo Settore) - (aggiornata al 19 settembre 2018).

*

Il tentativo fin troppo ambizioso di rendere chiare e immediatamente applicabili le norme del nuovo Regolamento UE 2016/679 *"relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"* e di spiegarne l'effettiva portata in ambito di volontariato e non profit cela sicuramente dei rischi non indifferenti.

Tuttavia, con il presente contributo si intende dare un concreto aiuto all'intero mondo associativo nell'affrontare il percorso di adeguamento al GDPR.

Premessa

Il nuovo Regolamento UE del Parlamento e del Consiglio Europeo 2016/679 detto **"General Data Protection Regulation"** (in breve **"GDPR"**) segna un'accelerazione ed anzi un completo cambio di prospettiva nel campo della riservatezza e del trattamento dei dati personali.

Con la definitiva esplosione dei social network, delle piattaforme informatiche e dei motori di ricerca, le persone fisiche barattano la loro riservatezza in cambio di beni e servizi, rendendo disponibili ai propri amici, al pubblico, alle imprese e alle autorità pubbliche, su scala europea e mondiale, innumerevoli informazioni personali.

La libera circolazione dei dati favorisce gli scambi, le relazioni sociali, la conoscenza, il confronto, ma cela anche considerevoli rischi. E' quindi essenziale che ogni persona debba essere posta in grado di avere il controllo su come i suoi dati, singoli o organizzati, vengano utilizzati, nell'ambito di un quadro europeo (e internazionale) di regole comuni.

Il GDPR non ha comportato l'abrogazione totale dell'attuale normativa italiana ("Codice in materia di protezione dei dati personali" di cui al D.Lgs. n. 196/2003) che è stata modificata con il decreto legislativo n. 101/2018.

Il legislatore italiano, in sede di emissione del detto Decreto ha provveduto ad integrare ed adeguare il vecchio Codice Privacy alla nuova normativa UE. **Il decreto in questione, approvato dal Consiglio dei Ministri in data 8 agosto 2018, è entrato in vigore il 19 settembre 2018.**

Tra le novità che interessano il presente contributo particolare rilievo assume il disposto dell'art. 2 sexies del decreto n. 101/2018 nel quale espressamente sono citati tra le materie per le quali "si considera rilevante l'interesse pubblico relativo a trattamentiinerenti le "attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci" e i "rapporti tra gli enti pubblici e quelli del Terzo Settore".

1. Definizioni art. 4 GDPR

L'art. 4 del GDPR si occupa delle **definizioni di concetti e principi** posti alla base della nuova disciplina europea. La norma assume rilievo centrale attesa l'introduzionedi nuove categorie di dati.

L'articolo 4, paragrafo 1, n. 1 ***(I),*** del Gdpr definisce il Dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile". Per stabilire l'identificabilità di un Interessato, il Gdpr suggerisce di considerare tutti i mezzi (come l'individuazione) di cui il Titolare o un terzo può ragionevolmente avvalersi per identificare detto Interessato, direttamente o indirettamente.

Gli Interessati possono essere associati ad identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati (quali gli indirizzi IP) a marcatori temporanei (cookies) o a identificativi di altro tipo (come i tag di identificazione a radiofrequenza) che possono lasciare tracce che, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili e per identificare gli Interessati (si veda considerando 30 del Gdpr).

Il Gdpr ha introdotto nelle definizioni nuove categorie di Dati, tra cui quelli genetici e biometrici. Ha inoltre espressamente definito i dati relativi alla salute (i "Dati sanitari"). L'articolo 4, paragrafo 1, n. 13 (II), del Gdpr definisce i dati genetici come quei Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di un Interessato che forniscono informazioni univoche sulla sua fisiologia o salute e che risultano dall'analisi di un suo campione biologico (i "Dati genetici").

L'articolo 4, paragrafo 1, n. 14 (III), del Gdpr definisce i dati biometrici come quei Dati personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di un Interessato che ne consentono o confermano l'identificazione univoca, come l'immagine facciale o i dati dattiloscopici (i"Dati biometrici").

L'articolo 4, paragrafo 1, n. 15 (IV), del Gdpr definisce i Dati sanitari come quei Dati personali attinenti alla salute fisica o mentale di un Interessato, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

2. Obiettivi del GDPR

Il GDPR vuole garantire in primo luogo 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) (V).

Un altro obiettivo fondamentale del GDPR è la libera circolazione dei dati. Questo obiettivo è fondamentale perché il GDPR non mira solo a tutelare un diritto fondamentale dell'individuo, ma a creare un terreno fertile per un'economia dei dati europea. Il GDPR si inserisce nel più ampio programma per un mercato unico digitale.

Più precisamente, il GDPR, si propone soprattutto di farsì:

a) che i dati personali vengano utilizzati per **scopi leciti** e comunque per le **finalità** in base alle quali sono stati raccolti e non oltre il tempo necessario per raggiungere tali finalità;

b) che i dati conosciuti da estranei, che non vengano diffusi **o comunque utilizzati contro la volontà o nell'ignoranza della persona cui si riferiscono;**

c) che i dati personali non vengano distrutti o perduti in modo involontario o doloso.

Il contesto delle nuove regole comunitarie è però anche quello del Digital Single Market (DSM) un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi, dei capitali – oltre che delle informazioni – in condizioni di piena concorrenza e di livello elevato di protezione dei consumatori e dei dati personali.

Un pilastro fondamentale del DSM è costituito dalla costruzione europea di un nuovo quadro regolatorio armonizzato in attuazione dei precetti contenuti nell'art. 7 (Diritto al rispetto della vita privata e familiare) (VI) e nell'art. 8 (Protezione dei dati di carattere personale) (VII) della Carta dei diritti fondamentali dell'Unione Europea.

3. Applicabilità del GDPR agli ETS

Gli ETS (Enti del cd Terzo Settore) raccolgono e utilizzano comunemente, nello svolgimento della loro attività, dati personali, e cioè informazioni e notizie riferite:

a) ai propri soci/aderenti;

b) ai beneficiari dell'attività istituzionale o utenti del servizio;

c) ai consulenti e collaboratori esterni;

d) agli eventuali dipendenti;

e) agli enti pubblici;

f) agli altri ETS e in genere i soggetti con cui vengono a contatto;

g) alle persone, enti e aziende a cui indirizzare campagne di sensibilizzazione e fundraising, ecc.

Costituiscono per esempio **raccolte cartacee** di dati personali il libro dei soci, il libro dei volontari, la rubrica per la corrispondenza, l'elenco dei donatori, ecc. Tali dati possono anche essere gestiti tramite computer e contenuti in **banche dati**, situazione che richiede l'adozione di particolari misure di sicurezza e di protezione dei computer.

Quanto alla natura dei dati, si ritiene di poter distinguere tra:

*—> **DATI PERSONALI "COMUNI"** (es. il nominativo, la data di nascita, il numero di cellulare dei soci/volontari o beneficiari, l'avvenuto versamento della quota associativa, gli studi compiuti), alcuni dei quali sono PUBBLICI, (es. il codice fiscale o le liste elettorali).*

*—> **DATI SENSIBILI**, che il GDPR chiama **"PARTICOLARI CATEGORIE DI DATI"***

*—> **DATI GIUDIZIARI***

Costituiscono dati personali (comuni o sensibili) anche le immagini, i suoni, i video ecc., quando consentono di individuare una determinata persona. Anche a tali dati, quindi, si applicano le regole del GDPR, oltre alle norme del codice civile (art. 10) (VIII) sulla tutela dell'immagine.

*

La normativa UE del GDPR si applica agli Enti del Terzo Settore, che sono **"titolari del trattamento"** se e ogni qualvolta svolgono anche una sola delle operazioni che concretano un trattamento di dati personali.

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.

È utile precisare che, ai fini dell'applicazione del Regolamento, le norme del GDPR che si riferiscono alle associazioni e agli ETS non distinguono tra i vari soggetti appartenenti al terzo settore, ma parlano genericamente di fondazioni, associazioni o organismi senza scopo di lucro.

Posto che per il GDPR il Titolare è la persona giuridica che decide che trattamento di dati svolgere e come svolgerlo ("determina le finalità e i mezzi del trattamento di dati personali") **si ritiene che debba esser considerata titolare del trattamento anche la sezione locale o l'organismo periferico di una associazione**, qualora appunto eserciti un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento.

In merito è necessario dare conto della definizione di *«stabilimento principale»*:

- *"per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, lo stabilimento principale è il luogo ove è situata la sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione*

di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale" (IX).

Alla luce della definizione sopra riportata ove la sezione / organismo locale di una associazione nazionale abbia il potere di decidere in autonomia le modalità e le finalità del trattamento di dati personali posto in essere, rispetto alla "casa madre", essi assumono la qualità di "titolare", e cioè soggetto autonomo ai fini dell'applicazione del GDPR e del rispetto degli obblighi conseguenti: dovrà pertanto predisporre una propria informativa, deve chiedere il consenso al trattamento, deve tenere se del caso i Registri del Trattamento e così via.

4. Principi e finalità nel GDPR

Ai sensi dell'art. 5 (X) gli ETS, come qualsiasi titolare:

*– devono trattare i dati in modo **lecito** e secondo **correttezza** e **trasparenza**;*

*– possono raccogliere i dati solo per **finalità** determinate, esplicite e legittime, ed utilizzare i dati solo in termini compatibili con tali scopi (**"limitazione delle finalità"**);*

*– devono assicurarsi che i dati raccolti siano adeguati, pertinenti e non eccedenti rispetto a quanto necessario per il perseguimento delle finalità per cui sono raccolti ("**minimizzazione dei dati**");*

*– devono avere dati esatti e, se necessario, aggiornarli ("**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 autorizz*ati o illeciti e per evitare la perdita e la distruzione accidentale dei dati ("**integrità e riservatezza**").

Il PRINCIPIO DI FINALITÀ, che resta anche per il Regolamento UE uno dei fondamenti del trattamento dei dati, implica che **la raccolta dei dati e il loro successivo utilizzo devono avere precise e determinate finalità, che vanno comunicate all'interessato e poi rispettate.**

Per gli ETS le finalità del trattamento dei dati generalmente coincidono o sono compresi **negli scopi istituzionali indicati nello statuto** (anche se lo statuto è spesso generico, ed invece le finalità del trattamento vanno nel dettaglio specificate nell'informativa).

5. Informativa ex art. 13 ex art 14 GDPR

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.

Ai sensi dell'art. 13 l'informativa deve contenere:

a) l'identità e i dati di contatto del ***titolare del trattamento*** *e, ove applicabile, del suo rappresentante;*
b) i dati di contatto del ***responsabile della protezione dei dati (Data Protection Officer o DPO)****, ove nominato;*

c) le ***finalità*** *del trattamento cui sono destinati i dati personali nonché la* ***base giuridica*** *del trattamento;*

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) (esistenza di un "legittimo interesse del titolare del trattamento o di terzi" che non leda i diritti e le libertà fondamentali dell'interessato), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Inoltre, la stessa informativa deve contenere:

a) il ***periodo di conservazione*** *dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;*

b) l'esistenza del ***diritto dell'interessato*** *di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;*

c) qualora il trattamento sia basato sull'articolo 6 ***(Liceita' del Trattamento)****, paragrafo 1, lettera a), oppure sull'articolo 9* ***(Trattamento di categorie particolari di dati personali)****, paragrafo 2, lettera a), l'esistenza del* ***diritto di revocare il consenso*** *in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;*

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

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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

In relazione alle modalità di "*consegna*" dell'informativa ed alla validità ed efficacia della medesima si prospettano le seguenti:

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

*– l'informativa può essere anche spedita **via e-mail**. In questo caso può essere opportuno chiedere al destinatario di rinviare un messaggio di "conferma", che l'ente potrà stampare o comunque conservare;*

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

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

L'informativa va comunicata/consegnata **ai soci e/o volontari, ai collaboratori esterni, ai dipendenti, ai beneficiari e a tutti coloro di cui l'associazione acquisisce, conserva e utilizza dati personali**, che si possono definire "*interessati*".

La comunicazione/consegna va fatta nel momento in cui l'interessato fornisce i suoi dati all'associazione: in pratica la prima volta che la persona viene a contatto con l'ente.

*

Se i dati non sono raccolti direttamente presso l´interessato l'art. 14 del regolamento, prevede le informazioni da fornire ed esattamente:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) le categorie di dati personali in questione;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

Oltre alle informazioni di cui al paragrafo 1, il titolare fornisce altresì le informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

c) 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 dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

d) 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 prima della revoca;

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

f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

In merito ai termini entro i quali fornire le informazioni di cui ai paragrafi 1 e 2 l'art. 14 prevede:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Al comma 4 la norma disciplina l'ipotesi di utilizzo di dati per finalità diverse da quelle per cui sono stati ottenuti e prevede che: "*prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2".*

Il comma 5 infine si occupa delle ipotesi di non applicazione dei precedenti commi da 1 a 4 prevendendo che:

"I paragrafi da 1 a 4 non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge".

6. Conservazione, aggiornamento e rettifica dei dati

In merito al tema della **conservazione dei dati,** si osserva che il GDPR, all'art. 9 comma 2 lett. d) (XI) consente l'utilizzo dei dati (*sensibili* leggesi *particolari*) degli ex soci anche senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'associazione e con adeguate garanzie (di protezione dei dati), con divieto però di comunicazione all'esterno (per tale comunicazione ci vuole il consenso specifico dell'ex socio). In applicazione del principio di proporzionalità e minimizzazione dei dati, i dati "trattenuti" dall'associazione dopo l'uscita del socio dovranno però essere strettamente inerenti alle specifiche attività "residue" (es. invio della newsletter, convocazione per eventi speciali, ecc.), e quindi potranno per esempio ridursi al nominativo e all'indirizzo mail.

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

E' chiaro interesse dell'associazione far sì che le informazioni relative ai soggetti con cui e a favore di cui opera siano aggiornati, e nella pratica ciò avviene comunemente, per iniziativa dell'associazione o dell'interessato che comunica all'associazione le variazioni intervenute (es. cambio di indirizzo).

L'aggiornamento/rettifica dei dati è anche un vero e proprio diritto dell'interessato.

Riassumendo:– ***nell'informativa di cui all'art. 13 GDPR andrà specificato quali dati l'associazione intende conservare anche dopo la cessazione del rapporto associativo****, fermo restando l'avvertimento all'interessato che comunque, in ogni caso, il socio cessato potrà chiederne la cancellazione (cd* ***Diritto all'oblio****);*

*– dei dati del socio cessato è comunque **vietata la comunicazione all'esterno o la diffusione** (salvo esplicito consenso del socio);*

*– con le opportune cautele per evitarne la diffusione, l'associazione potrà, secondo i principi di cui sopra, conservare una sorta di "**albo d'oro**" con i nominativi di coloro che sono stati soci, attraverso una rubrica o albo cartaceo (o attraverso lo stesso libro soci "storico") conservati in luogo non accessibile a terzi.*

7. Diritti dell'interessato

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

Una precisazione preliminare è d'obbligo. Va infatti chiarito che *l'interessato può esercitare i suoi diritti compatibilmente con le condizioni di liceità in base alle quali il titolare tratta i dati*…". La previsione normativa è chiaramente tesa ad effettuare un bilanciamento tra l'esigenza di protezione dei dati rafforzata attraverso i diritti riconosciuti dal GDPR ed il non rendere eccessivamente gravoso per i titolari il trattamento di dati in presenza di particolari condizioni di liceità.

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

– di avere conferma che l'ente utilizza i suoi dati e di sapere quali siano questi dati;

– di conoscere l'origine dei dati (cioè come e da chi l'ETS li ha acquisiti), le finalità del trattamento, i soggetti a cui i dati vengono comunicati e il periodo di conservazione dei dati;

– di rettificare (correggere o integrare) i dati inesatti o incompleti (es. cambio di indirizzo o dello stato civile, aggiornamento del curriculum, ecc.);

*– di cancellare i dati (cd. **diritto "all'oblio**") quando il trattamento non è più necessario per il raggiungimento delle finalità per cui sono stati raccolti, o in caso di revoca del consenso, o in caso di trattamento illecito o negli altri casi previsti dall'art. 17 GDPR;*

– di ottenere una "limitazione del trattamento" nei casi previsti dall'art. 18 GDPR;
*– di poter trasferire i dati ad un altro titolare (diritto "alla **portabilità** dei dati");*

– di opporsi al trattamento dei suoi dati, anche se svolto correttamente dall'associazione, se sussistono "motivi particolari" (cioè particolari e valide ragioni: ad esempio se ha presentato domanda di recesso dall'associazione, o se il trattamento, anche se lecito, risulta lesivo della sua dignità o riservatezza);

*– di opporsi al trattamento dei dati svolto per il "**marketing diretto**" (invio di materiale pubblicitario o vendita diretta o compimento di ricerche di mercato o di comunicazione commerciale);*
– di non essere sottoposto ad una decisione basata su un "trattamento automatizzato" di dati (inclusa la cd. Profilazione).

Quindi **ogni persona può chiedere ad ogni titolare** (anche agli ETS) **se e in che modo utilizza suoi dati personali e di esercitare i suddetti diritti.** Tale richiesta che potrà pervenire tramite lettera raccomandata, fax o posta elettronica.

8. Dati particolari

L'art. 9 del GDPR (XIV) si presta ad alcune importanti considerazioni ed in particolare prendendo le mosse dalla formulazione testuale del comma 1, risulta di tutta evidenza in primo luogo un espresso divieto di trattamento di tutti quei dati che, oltre la soglia dei dati comuni, identificano il soggetto nella sua dimensione fisica e altresì in quella sociale contribuendo alla de-costruzione del prisma unitario dell'identità personale, per individuare le molteplici dimensioni della persona Il comma I, se nella prima parte richiama quanto previsto dall'art. 8 della Direttiva 95/46, con riferimento ai dati personali che rivelino l'appartenenza razziale o etnica o le convinzioni religiose e filosofiche, le opinioni politiche o l'appartenenza sindacale, se ne discosta quando contempla "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". L'ambito delle categorie contemplate è davvero molto ampio: basti considerare i dati genetici, nonché i dati "dati biometrici"; tali categorie chiamano in causa, quanto a modalità e finalità di trattamento, diverse considerazioni in ordine non soltanto ai soggetti che possono essere a ciò preposti, ma anche in ordine alla valutazione preventiva ed ai protocolli di sicurezza che dovranno essere adottati nel trasferimento e nella circolazione dei dati. Se il comma 1 esordisce ponendo il divieto di trattamento con riferimento alle categorie di dati considerati, il comma seguente prevede una serie di eccezioni, che legittimano o rendono lecito il trattamento: nelle lettere da a) a j) vengono infatti individuate una serie di circostanze (sottratte all'applicazione del divieto) che possiamo raccogliere individuando tre macro-categorie, collegate all'interesse per la realizzazione/tutela del quale, le attività di trattamento vengono consentite. Una prima categoria può individuarsi con riferimento alle ipotesi nelle quali rileva un interesse individuale del soggetto dei cui dati si tratta e cioè che il soggetto abbia dato il suo consenso esplicito per una o più finalità (lett. a), che il soggetto abbia reso manifestamente pubblici quei dati (lett. e) oppure sia in considerazione un interesse vitale dell'interessato o di altra persona fisica e l'interessato sia in stato di incapacità e non possa prestare il proprio consenso (lett.c).

Una seconda categoria con riferimento all'interesse del titolare del trattamento e dell'interessato, cioè quando il trattamento sia necessario per "assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale" (lett.b); od ancora quando sia effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, con la duplice condizione 1) che l'ente agisca nell'ambito delle sue legittime attività e 2) con adeguate garanzie e che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità; nonché con l'ulteriore considerazione del divieto di comunicazione all'esterno senza il consenso dell'interessato (lett. d).

Una terza e più ampia categoria può individuarsi con riferimento a tutte le altre ipotesi, che riguardano situazioni di interesse generale, collegate all'attività di giustizia (lett. f.), all'esistenza di un interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, sempre nel rispetto dei principi di finalità e non eccedenza (lett. g), ed alle attività svolte a fini "di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" (lett. j); sempre in questa ampia categoria possono ricondursi le ipotesi previste alle lettere h) ed i), poste a tutela di interessi correlati alla tutela della salute, sia in dimensione individuale che collettiva, anche come prevenzione per il rischio di epidemie o diffusione di nuove patologie trattamento è necessario a fini di archiviazione nel pubblicoparagrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi.
Il GDPR contiene, al citato art. 9, una definizione (piuttosto generica) di "**categorie particolari di dati personali**", che comprendono:

– ***DATI SENSIBILI****, che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale";*

– ***DATI GENETICI*** *e* ***DATI BIOMETRICI*** *intesi a identificare in modo univoco una persona fisica;*

– ***DATI SANITARI*** *(e cioè i dati relativi alla salute) o quelli relativi alla vita sessuale o all'orientamento sessuale della persona.*

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

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

9- Dati Giudiziari dopo paragrafo dati particolari

Il GDPR regola i dati giudiziari all'art. 10, stabilendo che *"il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.*

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".

10. Condizioni di Liceità del trattamento

In merito alle basi giuridiche del trattamento deve necessariamente richiamarsi il disposto dell'art. 2 sexies del decreto n. 101/2018 (XV) nel quale espressamente sono citati tra le materie per le quali "si considera rilevante l'interesse pubblico relativo a trattamenti inerenti le "attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci" e i "rapporti tra gli enti pubblici e quelli del Terzo Settore".

L'impatto della nuova disposizione è decisamente significativo consentendo il trattamento delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

La norma considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie inerenti le "attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci" e i "rapporti tra gli enti pubblici e quelli del Terzo Settore".

Al di la' di quelli che potranno essere gli effetti della nuova base giuridica di trattamento di cui al citato art, 2 sexies il Codice Privacy stabilisce che **se l'ente non profit tratta i dati personali comuni e sensibili dei soci per gli scopi statutari e non li comunica a terzi e non li diffonde, non ha l'obbligo di acquisire il consenso / autorizzazione dei soci.**

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

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

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

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

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

*– è necessario per l'**esecuzione di un contratto** del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;*

*– è necessario per l'esecuzione di **compiti di interesse pubblico**;– è necessario per il perseguimento del **legittimo interesse del titolare del trattamento o di terzi** che non lega i diritti e le libertà fondamentali dell'interessato (es. le campagne di raccolta fondi).*

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

– è necessario per gli adempimenti in materia di diritto del lavoro, sicurezza sociale e protezione sociale;

– è necessario per tutelare un interesse vitale dell'interessato o di altra persona fisica, e costoro non possano prestare il consenso;

– riguarda dati "resi manifestamente pubblici dall'interessato".

Le norme di cui sopra consentono quindi agli ETS di **non chiedere il consenso** se il trattamento:

*– dei dati comuni e sensibili è necessario per l'adempimento degli obblighi nascenti dal **rapporto di lavoro** con i propri dipendenti;*

– consiste nella comunicazione obbligatoria dei dati comuni all'Agenzia delle Entrate;

*– consiste nella comunicazione dei dati comuni degli associati alla compagnia di assicurazione da parte delle ODV ed ETS iscritti ai registri del volontariato (e in futuro al RUNTS) per l'**assicurazione obbligatoria**;*

– di dati comuni serve per eseguire un servizio richiesto dal beneficiario (es. richiesta di trasporto o assistenza domiciliare);

– di dati particolari/sensibili serve per la tutela della vita o incolumità fisica della persona;

– di dati comuni avviene per campagne di raccolta fondi (fermo restando il diritto dell'interessato di opporsi).

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

E va comunque tenuto presente:

*– che anche in caso di esonero dal consenso, **va sempre fornita all'interessato l'informativa**, nella quale descrivere specificamente le modalità con cui l'associazione utilizza i dati;*

*– che **i dati sanitari** e quei dati idonei a rivelare la vita sessuale **non possono essere diffusi nemmeno su consenso dell'interessato.***

*****

Ecco le **caratteristiche del consenso** descritte all'art. 7 (XVIII) del GDPR:

*– **espresso**, cioè esplicito e manifestato in modo inequivocabile (non può essere desunto da un comportamento indiretto);*

*– **libero**, cioè manifestato liberamente dal soggetto, richiesto in termini non definitivi e non incondizionati. Inoltre, il consenso non può essere imposto se invece è facoltativo (ad esempio l'associazione non potrà imporre all'aderente di prestare il consenso al trattamento dei suoi dati per finalità estranee all'associazione, pena la sua mancata iscrizione);*

*– **specifico**, ovvero riferito ad uno o più trattamenti individuati e aventi specifiche finalità, e descritti con linguaggio semplice e chiaro;*

*– **informato**, ovvero preceduto dall'informativa di cui all'art. 13;*

*– **sempre revocabile** (ovviamente la revoca non comporta l'illegittimità dei trattamenti svolti in precedenza).*

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

Si possono a tal proposito utilizzare degli accorgimenti quali:

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

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

*– se l'associazione gestisce un sito web esiste la possibilità di utilizzare il cd. **point&click**, ovvero di creare attraverso appositi software una pagina web nella quale l'interessato può accedere (anche utilizzando una password appositamente comunicata dal titolare), per fornire i propri dati personali, per essere informato delle modalità del trattamento, e soprattutto per autorizzare il trattamento barrando una o più caselle (**che non sia già "preflaggate"**).*

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

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

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

Con riferimento agli interessati che siano **minorenni, il consenso va prestato da coloro che esercitano la responsabilità genitoriale** o, se esiste, dal tutore. **Il GDPR prevede espressamente che il consenso possa essere rilasciato dai minori che abbiano almeno 16 anni, ma, deve ritenersi, solo con riferimento all'offerta diretta di servizi della società dell'informazione"** (che sono quei servizi definiti all'articolo 1, par. 1 lett. b) della *Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione* - - come i servizi forniti "a distanza, per via elettronica e a richiesta individuale": le piattaforme web, Facebook, Dropbox, i Cloud, ecc.).

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

11. La figura dell'autorizzato al trattamento

La figura dell'Autorizzato, (o Incaricato come era indicato dalla disciplina previgente) del Trattamento è in base all'attuale Codice italiano obbligatoria (art. 30), ma non è espressamente prevista dal GDPR, che all'art. 29 (XIX) fa solo riferimento a *"soggetti istruiti"* dal titolare del trattamento.

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

Quindi è utile e anzi necessario continuare a rispettare i seguenti accorgimenti:

– gli incaricati/autorizzati operano sotto la diretta autorità del Titolare, attenendosi alle istruzioni impartite;

– la nomina/ designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito;

– la nomina degli incaricati/autorizzati, con le opportune istruzioni, è ***necessaria anche se la persona esegue solo trattamenti "cartacei" e non informatici.*** *Quando la persona utilizza il computer, la sua designazione e la delimitazione del suo trattamento rientra nel cd. sistema di autorizzazione;*

*– il titolare potrà consegnare all'incaricato/autorizzato un documento (**contratto e/o lettera di incarico)** nella quale lo designa come tale, indica che trattamenti egli può svolgere, su che dati, con quali modalità e nel rispetto di quali misure di sicurezza. Se l'incaricato/autorizzato svolge un trattamento informatico i "confini" del saranno corrispondenti al "profilo di autorizzazione".*

Infine, sempre ai fini della dimostrazione di aver adottato tutte le MISURE ADEGUATE, va assicurata la formazione degli Incaricati/autorizzati sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili del GDPR più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano.

12. La nuova figura del DPO

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

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

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

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

a) gli enti pubblici;

b) i (Titolari) privati che hanno come attività principale lo svolgimento di "trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala";

c) i (Titolari) privati la cui attività principale consiste "nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

Il concetto di "larga scala" appare meritevole di approfondimenti. Infatti, all'interno dell'articolo 37, paragrafo 1, lettere b) e c) del Regolamento, non si dà alcuna definizione di trattamento su larga scala.

Un importante contributo in materia è stato dato da "Gruppo di lavoro ex Articolo 29" o anche "WP 29" (da "Working Party art. 29"), istituito dall'art. 29 della direttiva 95/46.

Si tratta di un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.

Questo Gruppo ha emanato delle linee guida adottate il 13 Dicembre 2016 e riviste ed emendate in data 5 Aprile 2017 sul Responsabile della Protezione Dati proprio per dare indicazioni su elementi del Regolamento che sono lasciati in forma generale, tra cui il concetto di "larga scala", spiegando che: *è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; […]*

il WP 29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

- la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento.

In seguito, nelle linee guida, vengono elencati alcuni dei casi in cui è necessario dotarsi di un DPO: trattamento di dati sanitari svolto da un ospedale, dati di geolocalizzazione raccolti in tempo reale per finalità statistiche, dati relativi a clienti in ambiti assicurativi o bancari, e via così.

Il WP 29 suggerisce l'adozione di standard che permettano una determinazione quantitativa certa, ma per ora questi standard non sono ancora stati scelti. Quindi, in via interpretativa, saranno da considerare tutti i fattori sopraelencati: numero soggetti interessati, volume dei dati, tipologia dei dati, durata dell'attività di trattamento, estensione geografica del trattamento. Se uno di questi fattori rientra nei termini di "larga scala", ossia, interpretando in maniera negativa, se non è un trattamento locale, limitato nel tempo, su dati non sensibili, e su un numero limitato di persone, sarà possibile per un privato evitare di nominare il DPO.

In sostanza ogni azienda dovrà quantificare in base ai parametri suddetti se rientra o meno in un concetto di "larga scala", e in base a questo risultato dovrà decidere se il proprio trattamento dei dati richieda o meno la nomina di un DPO. Per poter arrivare a questo risultato è necessario in tal senso impostare un'analisi dei rischi, che quantifichi le richieste del regolamento, analizzi accuratamente le tipologie di dati trattati, le categorizzi, e valuti se queste richiedano o meno la figura del Responsabile della protezione dei dati.

Anche il "monitoraggio regolare e sistematico degli interessati" è un concetto piuttosto vago che non trova definizione all'interno del GDPR; tuttavia, il considerando 24 (XXI) del Regolamento menziona il "monitoraggio del comportamento di detti interessati" ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet, anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

A giudizio del WP 29 l'aggettivo "regolare" ha almeno uno dei seguenti significati:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;

ricorrente o ripetuto a intervalli costanti;

- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati, a giudizio del WP29:

- che avviene per sistema;

- che è predeterminato, organizzato o metodico;

- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;

- che è svolto nell'ambito di una strategia

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

Le Linee Guida europee (Article 29 Data Protection Working Party) hanno indicato a titolo esemplificativo come soggetti che svolgono trattamenti su vasta scala gli ospedali, le aziende di trasporto, le compagnie assicurative e gli istituti di credito, i fornitori di servizi di telecomunicazione, ecc.

Fin qui sono stati analizzati i casi di obbligatorietà di nomina di un DPO ai sensi del GDPR, ma il WP 29 si spinge anche più in là, raccomandando a titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un DPO, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

Tale analisi fa parte della documentazione da presentare, su richiesta, all'Autorità Garante per la protezione dei dati, in caso di verifiche, controlli ed ispezioni.

La documentazione sulla facoltatività e quindi sulla mancata adozione del DPO deve essere aggiornata ove necessario, per esempio se i titolari o i responsabili intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'art. 37, paragrafo 1.

Nel caso in cui invece il titolare o il responsabile optino per la nomina di un DPO su base volontaria, troveranno applicazione tutti i requisiti di cui agli artt. 37-39 (XXII) per quanto concerne la nomina stessa, lo status e i compiti del DPO, esattamente come nel caso di una nomina obbligatoria.

Nulla osta, precisa il WP 29, a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un DPO e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali.

In tal caso è fondamentale però garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di Responsabile per la protezione dei dati (DPO), ma come semplici consulenti.

Queste considerazioni valgono anche per i Chief Privacy Officers (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, per esempio, le risorse disponibili o la salvaguardia della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "DPO".

Si tenga presente che la designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'UE.

Occorrerà quindi aspettare e vedere se il legislatore italiano od europeo prevederà ulteriori casi di estensione dell'obbligatorietà.

13. Misure Tecniche ed organizzative adeguate

Il nuovo regolamento Europeo lascia ampi margini di azione a chi detiene la Responsabilità del trattamento. La protezione delle informazioni e dei loro trattamenti è basata su un approccio "Risk based", concetto per il quale tutte le misure tecniche o organizzative di sicurezza devono essere adeguate al rischio riscontrato ed analizzato presso il titolare del trattamento.

È questo il nuovo approccio europeo: da un lato lascia ampio raggio di libertà nell'applicare le misure di sicurezza, dall'altro impone, ad ogni singola realtà aziendale, pubblica e privata, di qualsiasi dimensione, di prevedere un'attenta analisi del rischio, così da poter adeguare le scelte operative e gestionali a tutela del dato.

A comandare questo processo è il principio dell'"accountability" secondo il quale il titolare del trattamento è tenuto a mettere in atto tutto ciò che ritiene necessario per poter garantire e dimostrare la conformità delle attività di trattamento con il regolamento stesso, compresa l'efficacia delle misure.

Il Codice Privacy esplicitava, in maniera dettagliata, nel suo più importante allegato (allegato B), quali dovessero essere le misure tecniche da adottare sia a livello informatico che non, per potersi ritenere a norma.

Tutte le misure adottate dovevano essere aggiornate periodicamente per adeguarle alle nuove esigenze organizzative o a un mutato livello di rischio.

L'approccio del nuovo regolamento risulta essere molto più astratto e come anticipato, lascia libertà di adeguamento allo stesso titolare, che dovrà garantire un "adeguato" livello di sicurezza dei dati oggetto di

trattamento, e dimostrare che lo stesso trattamento avvenga in conformità del regolamento europeo. L'articolo 24 (XXII)del GDPR prevede che:

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Nell'articolo successivo del nuovo regolamento, si introducono delle nuove tecniche di sicurezza che non troviamo nella nostra attuale normativa, e cioè pseudonimizzazione e minimizzazione. La pseudonimizzazione o semplicemente cifratura, consiste nell'utilizzare una chiave di cifratura per rendere illegibili i dati da parte di utenti malintenzionati.

Va chiarito però che la necessità di cifratura dei dati deve essere commisurata all'analisi effettuata sul rischio reale del trattamento la normativa europea sottolinea, soprattutto nei considerando (75) (XXIII), come debbano essere i progettisti di applicativi concernenti il trattamento dei dati, a mettere a disposizione, del titolare del trattamento, strumenti adeguati di cifratura. Ed è così che la scelta effettuata dagli stessi Titolari cadrà obbligatoriamente sui brand che utilizzano un occhio di riguardo nello sviluppo di procedure cifrate.

La richiesta normativa ha quindi un duplice scopo: da un lato contribuisce a sensibilizzare i titolari sull'argomento, dall'altro favorisce, nello sviluppo tecnologico, il miglioramento delle tecniche di sicurezza informatiche applicate nelle varie procedure.

Il GDPR non prevede che le misure di sicurezza siano definite dalla legge o da un documento tecnico, ma **assegna al Titolare la totale responsabilità di individuare tutte le MISURE TECNICHE E ORGANIZZATIVE ADEGUATE alla propria attività**, tenendo conto:

– dello stato dell'arte e dei costi di attuazione;

– della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento
– dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche
e ciò al fine:

– "di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente" al GDPR";

– "di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento";

– di assicurare "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico";

– di assicurare "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

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

*– l'adozione e il costante aggiornamento di prassi, procedimenti, strumenti tecnici e informatici specifici e prestabiliti, e cioè previsti e posti in essere prima dell'attività di trattamento (cd. **PRIVACY BY DESIGN**);*

*– che tali accorgimenti siano introdotti quale "impostazione predefinita" del sistema, tale che un trattamento non conforme sia rifiutato dal sistema (cd. **PRIVACY BY DEFAULT**);*

*– la redazione e conservazione di idonea **DOCUMENTAZIONE** (es. linee guida o regolamenti interni, contratti scritti di incarico con la ditta di software, istruzioni operative, ordini di servizio, ecc.) che valga a dimostrare verso l'esterno di aver approntato tali misure.*

*****

A titolo esemplificativo le **MISURE ADEGUATE** possono essere individuate come segue:

a) innanzitutto, non c'è dubbio che qualsivoglia trattamento informatico di dati non possa ormai prescindere dall'adozione delle vecchie "misure minime", e cioè dalla predisposizione:

*– di un sistema di **AUTENTICAZIONE INFORMATICA (A.1.)**, di **AUTORIZZAZIONE (A.2.)** e di **PROTEZIONE (A.3.)** del sistema informatico da virus e accessi indesiderati, al fine di "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"*
*– un sistema di conservazione dei dati attraverso **COPIE DI SICUREZZA**, per poter "ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".*

*

A.1 Autenticazione informatica

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

I codici di identificazione più semplici sono quelli basati sul sistema username e password; i più sicuri sono invece quelli che sfruttano le caratteristiche biomediche (voce o impronta del pollice).

L’username non può essere assegnato a diversi incaricati/autorizzati, nemmeno in tempi differenti. Quanto alle password, generalmente sono determinate pensando alla data di nascita, ai familiari, a parole di senso comune. Tuttavia, queste password non sono sicure, perché facilmente decifrabili.

Valgono tuttora per le password le indicazioni del vecchio Disciplinare Tecnico, opportunamente integrate, e quindi è assai consigliato:

– che la password sia di almeno 8 caratteri (oppure del numero di caratteri massimo consentito dallo strumento elettronico), e non contenga elementi facilmente ricollegabili alla persona del suo utilizzatore/incaricato;

– che sia composta da numeri e lettere insieme (maiuscole, minuscole) e da simboli;

– che sia conosciuta solamente dall’incaricato e quindi memorizzata dall’incaricato/utilizzatore del computer o conservata in modo da impedire la conoscenza di estranei (es. busta chiusa in un cassetto chiuso, oppure conservata da una sola persona con opportune cautele);

– che sia personale e assegnata a più incaricati/autorizzati (non sono quindi ammesse password di gruppo);

– che sia sostituita/modificata dall’incaricato al primo utilizzo [nei sistemi informatici complessi] e, successivamente, almeno ogni sei mesi;

– che sia disattivato l’accesso dell’utente quando il possessore delle credenziali cessa dalla qualità di incaricato (es. ex dipendente o ex socio) o quando l’accesso non è più effettuato per un certo periodo (es. maternità o malattia di una dipendente, infortunio).

L’individuazione iniziale delle password e degli username è generalmente svolta da un soggetto esterno esperto informatico (il vecchio “AMMINISTRATORE DI SISTEMA”). Questa figura non è stata più riproposta nell’attuale Codice italiano (e nemmeno nel GDPR).

Ciò non toglie che, nei fatti, ci possa essere e anzi sia altamente consigliabile la nomina ed il suo intervento: si tratta infatti del tecnico o della ditta che adatta il sistema informatico alle esigenze del Titolare, suggerendo le MISURE ADEGUATE in relazione ai trattamenti (informatici) svolti dall’Associazione.

A.2. Autorizzazione informatica

Un sistema di autorizzazione informatica si ha quando il sistema informatico predisposto dal Titolare distingue due o più “profili”, ovvero due o più ambiti diversi in cui si svolgono i trattamenti elettronici di dati all’interno dell’associazione, qualora il Titolare decida che uno o alcuni Incaricati/autorizzati possano svolgere solo determinati trattamenti e quindi possano accedere solo ad alcuni ambiti o programmi o banche dati, secondo il proprio “profilo”.

I profili possono riguardare ciascun incaricato/autorizzato ma anche “classi omogenee” di incaricati/autorizzati, e devono essere individuati prima del trattamento.

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

A.3 Protezione informatica

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

Se il computer o la "rete" di computer dall'associazione viene collegata a internet o ha un programma di posta elettronica e contiene altresì dati personali (e magari anche sensibili), le misure da adottare dovranno essere più incisive.

Gli accorgimenti più importanti sono qui di seguito riassunti:

– un valido e aggiornato ANTIVIRUS;

– un FIREWALL (in inglese "porta antifuoco"), che consente di bloccare le intrusioni dall'esterno da parte di hacker o di software dannosi che utilizzano accessi particolari per recare danno ai computer o controllare ed estrarre le informazioni (spesso il FIREWALL è integrato nel ROUTER messo a disposizione dal provider di internet);

– l'AGGIORNAMENTO periodico dei programmi e sistemi operativi, volti a prevenirne la vulnerabilità e a correggerne i difetti, o la SOSTITUZIONE dei programmi operativi desueti;

– il salvataggio dei dati mediante COPIE DI SICUREZZA o BACKUP, e cioè nella loro memorizzazione in banche dati portabili, chiavette USB, dischetti o supporti rimovibili, da conservarsi in un luogo diverso da quello dove si trovano i computer che contengono i dati originali (per evitare, ad esempio, che un incendio possa distruggere entrambi). Si consiglia almeno di formare delle copie di backup contenenti le banche dati (es. dei soci) e i documenti principali (es. verbali di assemblea).

– DISTRUGGERE I SUPPORTI ESTERNI quando non sono più utilizzati o cancellarne definitivamente il contenuto quando sono utilizzati da altri soggetti.

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

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

- *la* ***PSEUDONIMIZZAZIONE****, la* ***MINIMIZZAZIONE*** *e la* ***CIFRATURA*** *dei dati personali;*

- *le misure tecniche e organizzative dirette a garantire che, "per impostazione predefinita", siano svolti solo i trattamenti di dati (per quantità di dati, periodo di conservazione e accessibilità) corrispondenti alle specifiche finalità del trattamento;*
- *le misure tecniche e organizzative dirette a garantire che, "per impostazione predefinita", non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*
- *l'adozione di una **PROCEDURA PER TESTARE**, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

14. Principi di Privacy by design e by default

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

Si può certamente in tale ottica osservare:
– vanno fornite istruzioni scritte agli incaricati/autorizzati per il controllo e la custodia degli atti e documenti contenenti dati personali;
– vanno individuati gli ambiti di trattamento dei dati consentiti agli incaricati/autorizzati a trattamento o a categorie omogenee di incaricati e il loro aggiornamento almeno annuale;
– va assicurato un accesso controllato agli archivi e documenti contenenti dati sensibili e/o giudiziari.

15. Registro delle attività di trattamento

All'art. 30 (XXIV) il GDPR prevede che i 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.

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

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

*

Ecco le principali caratteristiche del Registro:

– deve avere forma scritta, e quindi può essere un ***documento cartaceo*** *o un* ***documento/file elettronico*** *da stampare e conservare;*

– non deve essere comunicato a terzi ma ***conservato presso la sede****;*

– deve essere periodicamente ***aggiornato.***

*– non è indispensabile abbia "****data certa****", anche se in via cautelativa è certamente buona prassi inviarlo via pec a terzi, affinché sia possibile risalire con certezza (giuridica) al giorno in cui è stato redatto o aggiornato.*

Gli obblighi sopra riportati va precisato non si applicano alle imprese o organizzazioni 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.

16. Data Protection Impact Assessment

La DPIA (Valutazione di impatto) è una procedura che il DGPR prevede (art. 35) (XXV) come sostitutiva dell'obbligo del Titolare di notificare al Garante l'esistenza di particolari trattamenti di dati.

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

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

a) che svolgono una ***PROFILAZIONE DI DATI****, e cioè raccolgono e raffrontano dati in via automatizzata per compiere una valutazione sistematica e globale di aspetti personali delle persone fisiche, valutazione che poi comporta l'assunzione di decisioni che riguardano significativamente tali persone;*

b) che svolgono un trattamento ***SU LARGA SCALA*** *di dati personali "particolari" e giudiziari;*

c) che svolgono un'attività di ***SORVEGLIANZA*** *sistematica su larga scala di una zona accessibile al pubblico.*

Si tratta di ipotesi che difficilmente interessano gli Enti del Terzo Settore, ad eccezione del trattamento di dati sensibili e giudiziari, per il quale è necessario capire quanto tale trattamento si svolge SU LARGA SCALA.

17. Data Breach

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

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

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

 l'occultamento comporta gravi sanzioni (fino a € 10.000.000,00);

 la violazione dei dati, se non bloccata o rimediata, può causare danno all'interessato.

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

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

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

*c) di **conservare** un registro dei data breach che deve contenere le seguenti informazioni:*

- i dettagli relativi al data breach, ovvero informazioni inerenti le cause della violazione, il luogo nel quale essa è avvenuta e la tipologia dei dati personali violati;

- gli effetti e le conseguenze della violazione;

- il piano di intervento predisposto dal titolare;

- la motivazione delle decisioni assunte a seguito del data breach nei casi in cui:

a. il titolare ha deciso di non procedere alla notifica

b. il titolare ha ritardato nella procedura di notifica

c. il titolare ha deciso di non notificare il data breach agli interessati

Il Gruppo di lavoro ex art. 29 ("WP 29") ha adottato il 6 febbraio 2018 la versione definitiva delle linee guida sulla notifica delle violazioni dei dati personali (cd. "Data Breach") ai sensi del Regolamento UE n. 679/2016 (cd. "GDPR").

Nel documento in esame, il WP 29 ha ricordato che il Data Breach consiste in una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il WP29, riprendendo la distinzione già operata nel suo precedente parere 03/2014 sulla notifica delle violazioni dei dati personali adottato il 25 marzo 2014, suddivide la violazione dei dati personali in tre categorie:

– "Confidentiality breach": in caso di divulgazione o accesso non autorizzato o accidentale a dati personali;

– "Availability breach": in caso di alterazione non autorizzata o accidentale di dati personali;

– "Integrity breach": in caso di modifica non autorizzata o accidentale di dati personali.

Come detto ai sensi dell'articolo 33, primo comma, del GDPR, in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Il GDPR ammette che i titolari del trattamento possano non essere in possesso di tutte le informazioni relative alla violazione nelle 72 ore successive al suo verificarsi. In tale ipotesi, il WP29 ha chiarito che i titolari hanno la possibilità di comunicare entro il termine di legge all'Autorità di controllo la sola violazione subita, per poi fornire in un successivo momento tutte le informazioni richieste dal suddetto art. 33, corredandole con i motivi del ritardo.

Il WP29 ha illustrato, inoltre, uno scenario in cui il titolare del trattamento, venendo a conoscenza di una prima violazione, si ritrovi, prima della notifica, a rilevare altre violazioni simili, ma con cause diverse. In tal caso, a seconda delle circostanze, il WP29 ha chiarito che il titolare, invece di notificare ogni singolo Data Breach, potrà provvedere con un'unica notifica contenente le diverse violazioni, qualora tali violazioni riguardino le stesse categorie di dati e si siano verificate tramite le stesse modalità, in un arco temporale ristretto. Qualora, invece, le violazioni riguardino categorie diverse di dati personali e si siano verificate tramite differenti modalità, il titolare dovrà effettuare una notifica specifica per ciascuna violazione riscontrata, in conformità all'articolo 33 del GDPR.

Qualora una violazione dei dati personali coinvolga dati di persone fisiche in più Stati Membri, il titolare deve notificare la violazione all'Autorità di controllo capofila. Inoltre, l'articolo 27 del GDPR (XXVII) impone al titolare del trattamento (e al responsabile del trattamento) di designare un rappresentante nell'UE in caso di applicazione dell'articolo 3, comma 2, del GDPR. In tali casi, il WP29 raccomanda che la notifica sia fatta all'Autorità di controllo dello Stato membro in cui è stabilito il rappresentante del titolare del trattamento nell' UE.

Il WP29 sottolinea che il titolare del trattamento dovrà documentare tutte le violazioni che si siano verificate, indipendentemente dall'obbligo di notifica, al fine di poter dimostrare la conformità al GDPR del trattamento effettuato. Come previsto dall'articolo 33, comma 5, del GDPR, il titolare del trattamento deve registrare i dettagli relativi alla violazione, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Il GDPR non specifica un periodo di conservazione per tale documentazione. Qualora tali registrazioni contengano dati personali, spetta al titolare del trattamento determinare il periodo appropriato di conservazione conformemente ai principi relativi al trattamento dei dati personali e indicare base legale per il trattamento. La documentazione dovrà essere conservata, in conformità all'articolo 33, comma 5 del GDPR, nella misura in cui tale documentazione consenta all'Autorità di controllo di verificare il rispetto di tale articolo o, più in generale, del principio di responsabilizzazione.

Oltre a questi dettagli, il WP29 raccomanda al titolare di documentare la motivazione delle decisioni prese a seguito di una violazione. In particolare, se una violazione non è stata notificata, occorre documentare la motivazione circa tale decisione. Ciò dovrebbe ricomprendere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche. In alternativa, se il titolare del trattamento ritiene che sussistano le condizioni di cui all'articolo 34, comma 3, del GDPR, deve essere in grado di provare adeguatamente che sussistano tali condizioni.

18. Sistema Sanzionatorio

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

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

Soprattutto, quando il titolare è una associazione, che è una persona giuridica, sorge il problema di individuare la persona fisica responsabile penalmente, poiché la responsabilità penale può colpire solo persone fisiche, salvo casi particolari (di cui al D.Lgs. 231/01) che non riguardano la privacy.

A tal proposito si può dire che, all'interno dell'associazione, la responsabilità penale colpisce chi, sotto il profilo sostanziale, esercita il potere direttivo e ha preso le decisioni in materia di privacy (ad esempio ha

deciso che trattamenti svolgere e le loro modalità, o ha deciso che misure adeguate adottare). Quindi i membri del Consiglio Direttivo, il Presidente dell'associazione, il Delegato del trattamento o l'Amministratore di sistema eventualmente nominati sono le figure più "esposte"; il **Presidente** si potrà liberare da responsabilità dimostrando di aver conferito al Delegato (ex Responsabile interno, ad esempio un membro del Consiglio Direttivo) deleghe effettive in materia di privacy, cioè poteri decisionali e di spesa, e dovrà probabilmente dimostrare anche di aver vigilato sull'operato del soggetto delegato. Nel caso del **Delegato** o dell'**Amministratore di sistema** questa prova liberatoria sarà forse più difficile: egli potrà dimostrare che non gli erano state attribuite quelle funzioni il cui scorretto esercizio ha determinato il compimento di un reato, ma l'esistenza di istruzioni scritte del titolare potrebbero rendere questa prova più ardua. La ripartizione delle responsabilità all'interno dell'associazione è un aspetto molto delicato: si consiglia di attribuirle in relazione all'effettiva competenza e capacità delle persone.

*

Le **SANZIONI AMMINISTRATIVE** previste dall'art. 83 (XXVIII) 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.*

*– 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";*

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

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

È possibile che, nonostante le violazioni sopra descritte, il Garante limiti l'importo della sanzione in ragione della natura non profit del Titolare o delle ridotte proporzioni dell'Associazione?

Tale possibilità non è certa né probabile, tuttavia **il GDPR indica specifici elementi che possono provocare, anche l'applicazione di una sanzione di basso importo**:

– 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:

a) l'associazione se l'illecito è compiuto dai suoi dipendenti;

b) il proprietario della cosa che è servita a commettere l'infrazione (es. l'associazione quale proprietaria del computer);

c) la persona che aveva la vigilanza su chi ha commesso l'illecito, salvo non provi di non aver potuto impedire il fatto.

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

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

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

L'art. 166 (XIX) del Codice privacy è stato completamente novellato dal decreto 101/2018 e definisce in modo dettagliato i criteri di applicazione delle sanzioni amministrative pecuniarie di cui all'art. 83 GDPR, nonché i provvedimenti correttivi di cui all'art. 58 GDPR. Il Garante è l'organo deputato ad irrogare tali sanzioni e adottare tali provvedimenti.

In tema di illeciti penali è stato novellato l'art. 167 del vecchio Codice privacy e sono state aggiunte due nuove fattispecie di reato. È stata ampliata la casistica riconducibile a ipotesi di trattamento illecito di dati personali e previsto che il pubblico ministero informi senza ritardo il Garante, non appena abbia ricevuto la notizia di reato. Inoltre il nocumento, la cui natura giuridica è stata da sempre controversa (la precedente formulazione dell'art. 167 lasciava infatti aperta la strada all'interpretazione del nocumento come condizione obiettiva di punibilità e non di elemento oggettivo del reato), diventa senza dubbio elemento costitutivo del reato, in quanto la condotta si concretizza nell'arrecare nocumento all'interessato: è punito "chiunque, operando in violazione delle disposizioni in materia di protezione dei dati, arreca nocumento all'interessato (…)".

L'art. 167-bis introduce il reato di comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala.

L'art. 167-ter introduce il reato di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala.

19. La responsabilità civile

L'art. 82 (XXX) GDPR 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 un ETS viola le norme del Regolamento causando un danno a terze persone, potrà esser chiamate in causa dal danneggiato davanti al giudice civile per ottenere il risarcimento del danno patrimoniale e/o morale.

L'Ente risponderà con i propri beni e – se l'associazione non ha la personalità giuridica – con il patrimonio personale delle persone fisiche che hanno agito in nome e per conto dell'Associazione in ambito privacy