Fiscal News

n° 14 Maggio 2mila18

Rivista informativa a cura dell'ufficio fiscale della Presidenza nazionale

In questo numero…

SPECIALE: PRIVACY 2018

CENTRO SPORTIVO ITALIANO

SPECIALE PRIVACY 2018

Un approccio per le piccole società sportive dilettantistiche

Il 25 maggio 2018 scade il termine per adeguarsi alle nuove regole europee in materia di protezione dei dati personali. La disciplina è contenuta nel Regolamento UE 679 del 2016, noto anche come **GDPR** (General Data Protection Regulation).

In questa circolare commenteremo le principali novità introdotte dalla nuova normativa, con particolare attenzione alle piccole realtà sportive del nostro circuito associativo allo scopo di sensibilizzarle sull'importanza del tema e facilitarne la comprensione.

Privacy 2018: cosa cambia?

Gli obblighi in materia di protezione dei dati non sono una novità per imprese ed enti senza scopo di lucro. Prima del regolamento europeo, già l'ordinamento italiano aveva provveduto a disciplinare la materia con due successive disposizioni: la legge 675 del 1996 e il D. Lgs 196 del 2003. Peraltro, come precisato dal Garante della Privacy, la maggior parte degli adempimenti e delle misure previste dal GDPR è similare a quella già stabilita dalle normative domestiche. Dunque quali esigenze sono alla base di questo cambiamento e, soprattutto, cosa occorre fare per adeguarsi?

Rispondere al primo quesito è abbastanza facile (nei paragrafi successivi forniremo alcuni spunti di riflessione per affrontare anche il secondo): le tecnologie informatiche nel 2018 sono ben più potenti e performanti di quelle del 2003. Esse consentono di "profilare" minutamente gusti, preferenze, desideri, necessità e perfino le idee politiche, religiose e sociali di qualsiasi cittadino che sia anche utente della rete e dei principali social network. Come noto, la finalità principale di questi trattamenti è quella di proporre offerte di beni e servizi personalizzate in base al profilo degli utenti, massimizzandone la probabilità di acquisto. La cronaca informa, però, che questi enormi database vengono sovente "bucati" dall'azione di hacker e criminali informatici: i relativi dati distrutti, sottratti o ceduti. Talvolta anche pubblicati, a danno non solo di imprese ed istituzioni, ma anche di tantissime persone fisiche non sempre nemmeno consapevoli di essere parte di quel trattamento dati: un problema di diritti, insomma, e non secondario.

Se i principali destinatari della riforma europea sono le grandi società che trattano i Big Data, i Social Network, le Pubbliche Amministrazioni, ecc., essa riguarda, però, anche gli enti senza scopo di lucro. Per loro natura, tutte le organizzazioni non profit trattano dati personali e molte, tra esse, anche quelli a carattere sensibile: pensiamo alle organizzazioni sanitarie, ai sindacati, ai partiti politici. Ne è investito, necessariamente, anche il mondo dello sport dilettantistico. La buona novità è che adempimenti e misure per la protezione dei dati non saranno uguali per tutti, ma

dipenderanno dalla complessità e dal rischio, da valutarsi caso per caso. Piccole organizzazioni con attività a basso profilo di rischiosità, dovranno gestire adempimenti minori e viceversa!

Il principio di responsabilizzazione

Il GDPR pone al centro della nuova normativa il principio di responsabilità: qualunque organizzazione che tratta dati personali (*si ricorda che per dato personale si intende qualsiasi informazione riguardante une persona fisica identificata o identificabile tramite, ad esempio: il nome, un numero di identificazione, un dato relativo alla ubicazione, un identificativo online, etc.*) ancor più se sensibili, (*ossia dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, etc.*) deve fare tutto il possibile affinché tali dati siano richiesti, acquisiti e trattati lecitamente con correttezza e trasparenza ed impegnarsi, al massimo delle proprie possibilità, per proteggerli, evitando che finiscano in mani estranee, si perdano, si corrompano o vengano lasciati inutilmente in soffitta anche quando ormai non sono più utili.

Il regolamento europeo, quindi, non chiede "la luna"… ma mira a sensibilizzare i titolari (e, con esso, anche i suoi fornitori, dipendenti, collaboratori) affinché pongano il massimo della cura sui dati in loro possesso, ricordando, sempre, che dietro ad essi vi sono le vite, i diritti e le storie di persone in carne ed ossa.

Anche le sanzioni, decisamente più elevate rispetto al passato (fino a un massimo di venti milioni di euro ovvero il 4% del fatturato mondiale totale annuo) sono motivate dalla necessità di enfatizzare la sensibilità di enti ed imprese sulla necessità di cui stiamo parlando e potranno essere evitate dimostrando, in maniera documentata, l'impegno che le organizzazioni hanno profuso per evitare danni e malfunzionamenti.

Quanto sopra può essere sintetizzato con un'espressione molto efficace: "Il Gendarme della Privacy sei tu". Ed è esattamente questo che il GDPR chiede alle organizzazioni, anche del terzo settore. Vigilare, essere sensibili, documentando il proprio impegno verso i diritti di riservatezza dei propri soci ed iscritti.

Privacy by design: la protezione dei dati è su misura

Altro principio fondante della nuova normativa è che non esistono misure uguali per tutte le organizzazioni. In altri termini la nuova privacy è un abito che si confeziona a misura delle esigenze e caratteristiche dell'ente titolare del trattamento. Nel nostro caso, una ASD che gestisce, per finalità esclusivamente istituzionali, i dati personali dei soci e tesserati, comunicandone gli estremi esclusivamente all'ente di promozione/federazione di appartenenza, e utilizzando i recapiti di posta elettronica degli iscritti al solo fine di inviare loro una newsletter informativa dell'attività sociale ed altri comunicati istituzionali (ad esempio le convocazioni assembleari, i relativi verbali, rendiconti ecc.), deve solo redigere e consegnare – in

sede di iscrizione - agli interessati una adeguata informativa, acquisendone il relativo consenso e comportarsi di conseguenza, proteggendo costantemente i dati detenuti con le ben note misure di sicurezza informatica (antivirus, firewall, backup dei dati) e cartacea (detenzione dei documenti in stanze e cassetti chiusi a chiave). Si tratta di operazione di routine, già note e ampiamente diffuse.

D'altro canto, se la ASD utilizza gli stessi dati per finalità promozionali e commerciali, cedendoli anche a soggetti terzi, raccogliendoli e trattandoli attraverso siti internet, se pubblica su piattaforme web o social, nomi e foto di atleti – a maggior ragione se minori – oppure se svolge attività con persona dalle caratteristiche sensibili (es. diversamente abili, persone con problemi giudiziari, ecc.) allora il livello di guardia dovrà essere ben più elevato. L'associazione, infatti, dovrà acquisire anche il consenso specifico ai trattamenti in questione e chiedere l'intensa e fattiva collaborazione delle ditte esterne che forniscono i vari servizi internet, social, marketing, ecc., affinché i dati detenuti siano sempre protetti al massimo delle proprie possibilità, tenuto conto che i maggiori rischi dipendono proprio dalla detenzione in rete degli stessi e dal fatto che sono coinvolti fornitori e ditte esterne. Sarà necessario, per esempio, formare dipendenti e collaboratori dell'associazione sulle misure previste dal GDPR, siglare con i fornitori contratti in cui vengono negoziate apposite clausole di responsabilità in materia di trattamento e protezione dei dati, nei casi più complessi nominare un **DPO** (Data Protection Officer, ovvero il responsabile della sicurezza dei dati). Il **DPO** è un professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati. Viene designato obbligatoriamente quando si trattano, su larga scala, dati sensibili.
Questo, per dire che meno dati personali si trattano, meno fatica e complessità si dovranno sostenere per proteggerli e meno rischi si corrono.

La nuova privacy è un processo dinamico
Un corollario di quanto sopra affermato, è che adempiere alla nuova privacy non si risolve nella compilazione di formulari astratti destinati ad essere subito dimenticati in cassetti polverosi. Il GDPR chiede ai titolari del trattamento (gli enti sportivi dilettantistici nel nostro caso) di interrogarsi sempre sull'impatto che le nuove e diverse iniziative hanno sui dati personali trattati. Ad esempio, se si organizza un nuovo torneo e ciò esige la compilazione di uno o più elenchi contenenti dati personali, dobbiamo interrogarci se abbiamo necessità di redigere una nuova informativa e/o acquisire il consenso specifico degli interessati (perché, ad esempio, intendiamo comunicare allo sponsor che patrocina l'iniziativa i nominativi dei partecipanti per finalità promozionali); qualora siano coinvolte ditte esterne potrebbe essere necessario impegnarle contrattualmente al rispetto della normativa di tutela e protezione; ci toccherà valutare con attenzione fino a quando sarà necessario conservare tali dati, proteggendoli e aggiornandoli fintanto che li deteniamo, cancellandoli non appena possibile.

In soldoni, la nuova privacy non esige formulari standardizzati. Non è come la dichiarazione dei redditi ove tutti i contribuenti utilizzano la stessa modellistica compilando esclusivamente i campi di propria pertinenza.
Le procedure, anche quelle citate dalla norma (es. l'informativa) sono tutte personalizzate ed è vietato scriverle in "legalese". Al contrario esse debbono essere chiare, sincere, trasparenti e ben comprensibili. Sempre adattate al contesto cui si riferiscono, secondo una procedura di aggiornamento e valutazione dinamica.

Cosa iniziare a fare per essere in regola
Essere in regola con il GDPR, significa proteggere al meglio delle proprie possibilità i diritti di riservatezza delle persone che hanno a che fare con le nostre associazioni. Come già precisato, la nuova normativa stabilisce pochi dettagli sul come questo possa farsi, investendo le associazioni stesse del compito di farsene gendarmi, sulla base del presupposto che nessuno è in grado di proteggere meglio i dati personali di chi li ha acquisiti lecitamente e sa come utilizzarli.

Questo è per alcuni versi una semplificazione (no a moduli ipertrofici scritti in linguaggio tecnico o burocratico) ma per altri è una rivoluzione culturale che ha colto impreparata la maggior parte delle imprese (circa l'80% risulta ancora inadeguata) e la stragrande maggioranza delle realtà non profit italiane (oltre il 90%). Problematiche similari si sono presentate anche in altri paesi UE, convincendo i relativi Garanti della necessità di un periodo di tolleranza, prima di applicare le sanzioni agli eventuali trasgressori. Il ritardo generale nell'applicazione, si intuisce anche dalla mancanza di adeguata letteratura pratica in materia, soprattutto per le piccole realtà e per il non profit. Ciò nonostante è essenziale mettersi al lavoro subito per adeguarsi alle nuove esigenze di tutela.

Il registro dei trattamenti
Un modo tutto sommato originale ed interessante di approcciare la tutela dei dati è immaginare che essa somigli un po' alla borsa in cui ogni mattina riponiamo i nostri effetti personali (chiavi, smartphone, laptop, portafogli, carte di credito, documenti, contanti, ecc.) prima di uscire.
Ciascuno di noi è sufficientemente consapevole di cosa serve portarsi dietro per affrontare una giornata fuori casa. Inoltre, a seconda dei casi, decidiamo di lasciare una o l'altra cosa in base del tipo di impegno che ci attende: ad esempio non porto il laptop che uso per il lavoro se esco solo per andare a correre nel parco o vado a mangiare una pizza con amici.
Inoltre, in relazione ai rischi che suppongo di correre, assumo le necessarie misure per evitare furti, scippi, distrazioni. In metropolitana debbo stare certamente più attento, ma anche al bar non lascio incustodita la borsa. La stessa sensibilità che impegno per i miei effetti personali, debbo usarla per i dati delle altre persone che mi sono stati affidati con fiducia.

Un registro dei trattamenti è dunque simile ad una borsa in cui so cosa c'è, cosa mi serve e cosa eventualmente, a seconda dei casi, è bene levare e come proteggere dai rischi e dalle insidie del caso.
Esso non è obbligatorio, ma come la borsa dedotta nell'esempio, è certamente il metodo più comodo per portare in giro i propri beni. Non è necessario redigerlo con un software o su uno schema prestabilito. Ogni organizzazione può impostarlo nel modo che ritiene più chiaro ed utile per se stessa: l'importante è che funzioni!

Il registro dei trattamenti dovrebbe contenere, ad esempio, almeno questi campi:

- **dati personali che sono assolutamente necessari per l'iscrizione all'associazione**: nome, cognome, data e luogo di nascita, indirizzo postale, indirizzo mail dei soci/tesserati. Questi sono i dati essenziali per poter inoltrare agli iscritti le comunicazioni che leggi e regolamenti impongono in funzione del rapporto associativo (convocazione e partecipazione alle assemblee, invio della newsletter istituzionale, dei rendiconti e decisioni, di altre comunicazioni associative);
- **gli eventuali dati sensibili nelle ipotesi in cui venissero acquisiti** (ad esempio, se la ASD dovesse organizzare uno specifico torneo dedicato a persone diversamente abili o nelle carceri, ecc.);
- **quali sono le norme di legge che ci impongono di richiedere tali dati**: certamente l'art. 148 del TUIR e l'art. 90 della legge 289 del 2002 in quanto normativa di riferimento fiscale per le ASD che fruiscono delle agevolazioni di settore. Ma anche le norme e i regolamenti del CONI e delle federazioni ed EPS per quanto concerne l'iscrizione nel Registro CONI e il tesseramento degli atleti. Ultimo, ma non per importanza, lo statuto della ASD stessa;
- **supporti in cui sono contenuti i suddetti dati**: essi saranno riportati di solito nelle domande di iscrizione sottoscritte dai soci stessi, nel libro soci, nei modelli di tesseramento, nei verbali di consigli ed assemblee, nei sistemi informatici di tesseramento. Potranno essere gestiti in modalità cartacea e/o elettronica e dunque risiedere in cassetti, armadi, dischi rigidi, penne usb, cloud, ecc.;
- **soggetti terzi a cui dobbiamo comunicare obbligatoriamente tali dati in forza di legge o regolamenti anche sportivi**: tali sono, ad esempio, il CONI, le federazioni e gli EPS cui la ASD è affiliata, per le esigenze di tesseramento;
- **per quanto tempo dobbiamo conservare tali dati**: trattandosi di dati rilevanti ai fini fiscali essi andrebbero conservati per l'anno in cui sono acquisiti e per i successivi cinque, in corrispondenza al periodo di prescrizione generale previsto in materia fiscale. Successivamente, a meno che non sussistano altre differenti motivazioni, andrebbero cancellati;
- **quali sono le persone che possono accedere, leggere, modificare, correggere o cancellare tali dati**: certamente il legale rappresentante della ASD (presidente) e chi ne fa le veci in caso di impedimento (vicepresidente). Dati di carattere fiscale o amministrativo sono, normalmente, oggetto di trattamento anche da parte dell'amministratore e degli eventuali consulenti esterni. Così come anche dagli

addetti di segreteria dell'associazione, anche se svolgono tale importante ruolo in qualità di volontari. Tutte queste persone possono essere definite, "responsabili" o "incaricate" del trattamento. La loro identificazione è una questione di organizzazione interna dell'associazione, ma è bene effettuarla per sapere chi fa che cosa, sensibilizzando, formando e responsabilizzando gli attori del sistema.

- **quali imprese, enti, organizzazioni, ecc. collaborano, a vario titolo, al trattamento dati:** abbiamo citato già CONI, federazioni, EPS, gli eventuali consulenti amministrativi. Anche per la gestione istituzionale, non di rado capita che l'associazione si avvalga di terzi gestori per la pagina web, la pagina facebook o altri trattamenti in rete. Anche con questi fornitori è essenziale che l'associazione preveda, per iscritto, specifici obblighi a tutela del corretto trattamento e protezione dei dati dei propri iscritti;
- **quali sono le misure di sicurezza che abbiamo predisposto per tutelare i dati**: conservazione dei documenti cartacei in cassetti chiusi a chiave all'interno di locali accessibili ai soli incaricati, computer e altri device dotati di adeguata password, antivirus, firewall. Aggiornamento periodico del sistema operativo e dell'antivirus. Modifica programmata delle password, ecc.;
- **abbiamo rilasciato idonea informativa agli iscritti relativamente al trattamento che faremo dei loro dati?** Il GDPR obbliga il titolare del trattamento (nel nostro caso la società sportiva) a fornire agli interessati (gli iscritti/soci/tesserati) una informativa completa, sincera, trasparente e facilmente comprensibile di quali dati personali debbono essere trattati in funzione dell'iscrizione alla società, per quali finalità, con quali modalità, a chi debbono essere comunicati in forza di legge o regolamento, come sono conservati e tutelati e quali diritti ha l'interessato (verifica, correzione, cancellazione, ecc.). Se abbiamo riflettuto e compilato adeguatamente i precedenti campi del nostro registro dei trattamenti, saremo in grado di fornire una adeguata informativa agli iscritti, che potrà essere associata anche alla domanda di iscrizione al sodalizio (ad esempio nella pagina retrostante).
- **abbiamo richiesto ed ottenuto il consenso degli iscritti al trattamento dei dati?** Di solito il socio presta il consenso al trattamento dei dati personali apponendo la relativa firma in calce all'informativa di cui abbiamo parlato nel punto precedente. Ciò può ritenersi sufficiente per il semplice trattamento dei dati per finalità esclusivamente istituzionali di cui stiamo discutendo in questa circolare. Non lo è più, qualora l'associazione intenda utilizzare i medesimi dati per scopi commerciali o se intenda pubblicarli, ad esempio su un sito internet o su un social, comunicarli e cederli a terzi: in questi casi, occorre uno specifico consenso per ogni ultroneo utilizzo.

Cosa farà il CSI per aiutare comitati e società sportive nella gestione della nuova privacy

Le linee di orientamento esposte in questa circolare sono dirette ai piccoli sodalizi che gestiscono i dati dei propri iscritti per finalità di carattere istituzionale sportivo,

escludendo ogni proposito di utilizzo commerciale, di diffusione e di comunicazione a terzi (fatta eccezione i casi in cui la comunicazione risponde ad obblighi di legge). Come già precisato, la privacy è su misura (by design) e le semplici operazioni fin qui descritte sono sicuramente insufficienti laddove il sodalizio intenda utilizzare i dati acquisiti anche per finalità promozionali, condividendoli con soggetti terzi, oppure operando in casistiche caratterizzate da dati sensibili (sanitari, giudiziari, contenenti opinioni politiche, filosofiche, religiose, ecc.). Nei casi più complessi potrebbe essere consigliabile che il sodalizio nomini anche un **DPO** sebbene tale possibilità sia obbligatoria solo in particolari casi, ad esempio se sono trattati su larga scala dati a carattere sensibile.
Bisogna anche rammentare quanto detto in proposito del carattere "dinamico" non statico della privacy. Dal 25 maggio parte, perciò, un processo di continuo miglioramento della tutela e della sicurezza.

Per agevolare comitati e società affiliate, il CSI ha affidato ad uno studio legale, leader nel settore della privacy, il compito di adeguare i sistemi informatici di affiliazione e tesseramento e quello di organizzare eventi di formazione in materia che saranno progressivamente estesi agli organismi territoriali del CSI. Nei prossimi giorni renderemo disponibile, inoltre, un facsimile di registro dei trattamenti ed uno di informativa disegnati secondo le nuove esigenze espresse nel GDPR.

Cosa fare al più presto
- riflettere su quali sono i dati personali gestiti dall'associazione, su quali supporti sono trascritti o memorizzati, sulle persone che sono autorizzate a trattarli, comprese le ditte esterne che gestiscono eventuali siti internet, social o similari;
- contattare le eventuali ditte e i consulenti esterni ed acquisire il loro impegno alla protezione e tutela dei dati personali, meglio se documentato per iscritto (ad esempio per mail);
- aggiornare i sistemi operativi dei PC, i relativi antivirus e firewall, fare un backup di tutti i dati su supporto adeguatamente custodito e programmare salvataggi frequenti e sistematici degli stessi: il rischio di un "data breach" cioè di una perdita o di un deterioramento involontario delle informazioni è quello più frequente ed insidioso;
- aggiornare sistematicamente le password evitando i comuni errori che si commettono spesso nella gestione delle stesse (es. usare i nomi e cognomi o le date di nascita, lasciare la password in bella vista sullo screen del PC),
- scansire la documentazione cartacea contenente i dati personali e custodirla al pari di quella elettronica avendo cura di porre gli originali in cassetti chiusi a chiave, all'interno di locali non accessibili ai non autorizzati.

Fiscal News

Grazie per l'attenzione

Ufficio Giuridico e Fiscale
Dr. Francesco Tramaglino
Avv. Paola Metalli

CENTRO SPORTIVO ITALIANO