General Data Protection Regulation

Regolamento UE 2016/679

VADEMECUM

per il trattamento dei dati personali da parte del CTA e delle società sportive

CAMPIONATI E TORNEI DELL'AMICIZIA

CTA

INTRODUZIONE

Siamo tutti esterofili!

Verso metà primavera 2018 alcuni amici, associati al CTA, facevano questa considerazione in merito all'argomento *privacy*, che si era da poco ripresentato con vigore e che li stava preoccupando parecchio. Si erano posti la domanda: "Ma perché dobbiamo sottostare all'invasione di tutti questi termini in inglese?"

Cercando di difendere l'italiano, con l'aiuto del dizionario, tentarono di tradurre *privacy*, non trovando però un unico termine che potesse raggiungere l'obiettivo. C'erano almeno tre definizioni ugualmente valide: *riserbo, riservatezza* e *segretezza*. Si arresero dunque e si adeguarono a quanto facevano tutti: soprattutto convennero che la *privacy* avrebbe continuato a interessare e coinvolgere sempre di più il CTA.

Iniziammo così a pianificare il lavoro di interpretazione del Regolamento UE 2016/679 (di seguito "Regolamento" o "GDPR"), per la protezione dei *dati personali*, in modo da poter mettere in regola il CTA con quanto prevede, e ahimè impone. Fu subito chiaro che ciò avrebbe riguardato gli associati CTA dello staff che operano sia all'interno della sede sia in mobilità, in linea con l'organizzazione dell'associazione. Fu anche chiaro però che il Regolamento riguardava in pratica anche tutti coloro che risultino soci di società sportive e che partecipino alle attività proposte dal CTA.

Com'è noto per lo statuto CTA, il dirigente di una società che iscrive la propria squadra ad un campionato o torneo organizzato dal CTA, ne diventa automaticamente socio; inoltre lo rende responsabile per il soggetto collettivo (cioè la propria squadra) che partecipa alla competizione sportiva. E diventano soci CTA anche tutti i suoi giocatori. Cominciai allora a pensare all'applicazione del GDPR in un'ottica più generale che comprendesse anche le società sportive iscritte alle competizioni.

La normativa sulla privacy esisteva anche prima del GDPR e, in passato, le problematiche legate alla sua osservanza erano state già affrontate. Si trattava della precedente versione del Codice per la protezione dei dati personali, il D. Lgs. 196/2003 (Testo unico sulla privacy), che prevedeva, oltre a misure sostanziali, una serie di adempimenti formali per i quali eravamo ricorsi a soluzioni adottate da altri organismi che avevano affrontato il percorso prima di noi.

Addentrandoci nel GDPR ci apparve subito chiaro che, in questo caso, lo spirito era completamente diverso. Non si tratta infatti di una legge italiana promulgata per adempiere a una direttiva europea, ma di un regolamento europeo, e in quanto tale, da applicare in Italia così com'è (altro che esterofilia!). Il D. Lgs. 101 del 10/08/2018, che ne ha completato alcuni aspetti riscrivendo completamente il vecchio Testo unico sulla privacy, all'art. 1 rimanda direttamente al Regolamento, limitandosi ad integrarne alcuni aspetti. L'impronta europea quindi domina incontrastata: naturalmente il nuovo D. Lgs. 196/2003 e i provvedimenti del nostro Garante, anche precedenti

al GDPR, vanno tenuti in considerazione e aiutano a superare eventuali difficoltà nell'applicazione pratica del Regolamento.

Cosa intendo per spirito completamente diverso?

Leggendo il GDPR si vede subito che la "mano" del legislatore è un'altra, ma ancor di più si nota come tutto il Regolamento ruoti attorno al concetto di re*sponsabilizzazione* (*accountability*) e l'obiettivo sia principalmente sostanziale. La protezione dei dati personali - vedremo poi cosa si intende per dato personale - e la tutela alla loro libera circolazione, non vengono perseguite elencando una serie di misure da adottare, sia tecniche sia amministrative, in modo che, armonizzandosi ad esse, l'organizzazione possa ritenersi in regola.

Il GDPR ribalta il punto di vista: non è il Regolamento che dice cosa bisogna fare per essere in regola. Il Regolamento impone a ogni organizzazione - avente a che fare con persone fisiche - di studiare il modo migliore per conseguire gli obiettivi indicati dal GDPR stesso. In caso di problemi, l'organizzazione dovrà *dimostrare* di aver messo in atto quelle specifiche misure, tecniche, informative e formative, che lei stessa ha ritenuto idonee al conseguimento degli obiettivi, in base all'analisi dei trattamenti da lei effettuati, dal loro profilo di rischio, dall'attività svolta, dalle sue dimensioni, dalle sue possibilità a livello organizzativo, economico, ecc. E dovrà essere convincente, perché l'aspetto sanzionatorio, nel GDPR, non è stato certo trascurato!

Qualcuno allora provò ad obiettare che la nuova normativa fosse indirizzata solo al mondo del lavoro. Nulla di più sbagliato! Purtroppo, o per fortuna, riguarda tutte le attività svolte dalle persone fisiche nei settori più svariati: sportivo, ludico, culturale, religioso, educativo e naturalmente lavorativo. Si pensi ad esempio ai vari circoli in cui vengono svolti tornei di scacchi o di carte o le biblioteche con i soci frequentatori schedati: tutti si imbattono nella privacy. E in base alle dimensioni, alla specifica attività dell'organizzazione, ai trattamenti di dati effettuati, le misure da adottare saranno diverse.

Ma cosa fa scattare l'obbligo di rispettare il Regolamento?

In pratica basta richiedere il nome, il cognome e il numero di telefono, allo scopo di approntare una rubrica telefonica, in un'attività che non possa essere definita a carattere esclusivamente personale o domestico, per essere obbligati a sottostare alla normativa sulla privacy.

Tutto ciò perché vale il principio che un riferimento identificativo di una persona fisica (non giuridica) sia un suo "bene personale" e pertanto di proprietà della stessa! E in quanto bene di proprietà della persona, può essere raccolto e gestito esclusivamente garantendo il totale rispetto dei suoi diritti. Ma c'è di più. L'insieme dei dati trattati, ad esempio una rubrica telefonica, costituisce un patrimonio, di proprietà altrui, che l'organizzazione deve trattare con la cura e la diligenza richiesta a chi am-

ministri un bene di terzi, a lui affidato.

Appena capii questi aspetti del GDPR il mio punto di vista cambiò radicalmente: dal considerarlo un'inutile e dispendiosa scocciatura cominciai ad apprezzarlo, cercando addirittura di far comprendere agli altri le sue potenzialità. Ho sempre avuto una certa preoccupazione per come venissero trattati i miei dati personali e sapere che un regolamento li tuteli, può solo farmi piacere.

Credo sia questa la regola d'oro per essere *compliant* (a proposito di esterofilia!) cioè conforme al GDPR: trattare i dati degli altri come vorremmo fossero trattati i nostri.

Quando il Consiglio Direttivo ha votato perché mi occupassi del GDPR, ho accettato e mi sono messo al lavoro per dare un supporto reale anche alle società sportive. Con la predisposizione dell'accordo di contitolarità, delle informative congiunte e di questo vademecum, mi auguro di aver contribuito all'applicazione del GDPR e di aver reso più semplice l'adeguamento a tutti coloro che partecipano alle attività del CTA.

Perché la *responsabilizzazione* sia reale ed efficace, deve essere accompagnata dalla formazione. E allora entriamo nel vivo e andiamo a conoscere le principali definizioni che compaiono nel Regolamento.

DEFINIZIONI

Cosa sono i DATI PERSONALI per il GDPR

Massima attenzione alla distinzione tra "dato personale" e "dato particolare o sensibile".

DATO PERSONALE: è una qualsiasi informazione, o combinazione di informazioni, che possa rendere una persona fisica, identificata o identificabile (quindi direttamente o indirettamente); rientrano in questa categoria i dati anagrafici, l'indirizzo dell'abitazione, il numero di telefono, l'e-mail (qualora contenga, ad esempio, il nome e il cognome), un codice personale (il codice fiscale, ma non solo quello), le fotografie (laddove il soggetto sia riconoscibile), il profilo sui social, il certificato medico che attesta l'idoneità all'attività sportiva , ecc.

Questi dati possono essere richiesti e devono essere trattati con cura.

DATO SENSIBILE: è un'informazione che rivela aspetti più intimi della persona, quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filoso-

fiche, il suo stato di salute, l'orientamento sessuale, l'appartenenza sindacale, la sua situazione giudiziaria, ecc.

Questi dati non possono essere richiesti e trattati, a meno che non ricorrano i casi previsti dall'art. 9 c. 2 del GDPR oppure sotto il controllo dell'autorità pubblica per quelli giudiziari.

Chi è l'INTERESSATO?

È la persona fisica alla quale fanno riferimento i dati, cioè il proprietario.

Chi è il TITOLARE (Data Controller)

È la persona o l'organizzazione che è in possesso dei dati dell'Interessato e decide in autonomia come trattare quei dati personali.

Il Titolare può avvalersi della collaborazione di altri soggetti, definiti genericamente Destinatari, che possono essere Contitolari (in virtù di un accordo interno, scritto, tra due o più Titolari, come quello in essere tra la società sportiva e il CTA) oppure Responsabili del trattamento (Data Processors), cioè persone od organizzazioni esterne che trattano i dati per conto del Titolare, da nominare a mezzo contratto o altro atto giuridico (è il caso, ad esempio, dell'azienda che offra un servizio di archiviazione, alla quale il Titolare affida i dati, mantenendone però il controllo). Anche in quest'ultimo caso è importante mettere per iscritto il contratto, sia per i nuovi rapporti, sia per quelli già in essere con i Responsabili del trattamento.

Attenzione a non confondere i Responsabili del trattamento con il Responsabile della protezione dati (RPD o DPO in inglese): quest'ultimo non è richiesto in piccole organizzazioni come le nostre.

Cos'è il TRATTAMENTO

È l'attività che viene svolta sui dati personali dell'Interessato da parte del Titolare (o chi per lui). Rientrano nel concetto di trattamento: la raccolta, la registrazione, l'organizzazione, l'archiviazione, l'utilizzo, la consultazione, la pubblicazione, la cancellazione, la distruzione, ecc. dei dati.

Il trattamento deve essere effettuato nei limiti di liceità, correttezza ed indirizzato allo scopo per cui sono stati richiesti i dati all'Interessato; può avvenire in forma cartacea, informatizzata o telematica.

Quali dati possiamo tenere e per quanto tempo

I dati personali devono essere raccolti nei limiti di quanto serve allo scopo, quindi non può essere raccolto nessun dato personale che non sia strettamente necessario alle finalità del trattamento.

Il loro trattamento deve essere pari al periodo di tempo necessario a perseguire le finalità della raccolta dei dati o per adempiere a disposizioni normative (ad esempio i termini civilistici per la conservazione del libro soci).

Quali sono i DIRITTI DELL'INTERESSATO

L'Interessato deve essere messo a conoscenza dei suoi diritti.

L'Interessato ha diritto di chiedere al Titolare l'accesso, la rettifica e la cancellazione dei dati personali che lo riguardino, oltre alla loro portabilità (il loro trasferimento presso un altro Titolare indicato dall'Interessato).

Il Titolare del trattamento ha l'obbligo di eseguire le richieste dell'Interessato dandogliene conferma, in tempi rapidi, oppure comunicargli i motivi che ne impediscano l'esecuzione.

Nel caso in cui l'Interessato richieda la cancellazione dei propri dati al presidente della società sportiva che lo ha iscritto ad un campionato, in quanto membro di una squadra, il presidente potrà opporsi alla cancellazione.

Se l'Interessato rinunciasse alla partecipazione al campionato, il presidente procederà alla cancellazione, comunicando all'Interessato quali dati non possano essere cancellati, la motivazione e il tempo di conservazione (ad es. il nome e cognome rimarrà scritto nel libro soci fino al termine legale della sua conservazione).

Cos'è il CONSENSO

È la libera volontà, chiara, specifica, inequivocabile, da parte dell'Interessato, con la quale egli approva ed autorizza in modo evidente il trattamento dei propri dati personali.

Il consenso deve essere dimostrabile, quindi nella maggioranza dei casi è indispensabile sia scritto (non ha alcun valore se verbale, tranne quando ci sia una registrazione) e deve essere esplicito: sono senza valore clausole quali "per tacito consenso" o caselline già barrate anche se sotto di esse fosse apposta la firma.

Il Regolamento è molto attento ad evitare trucchi e sotterfugi: per questo impone che il modulo con il consenso sia a sé stante (cioè separato dal modulo di raccolta dei dati), scritto in forma chiara e comprensibile all'Interessato.

Il consenso dovrà essere specifico verso le finalità per cui i dati sono stati raccolti.

Che cos'è l'INFORMATIVA

È il documento con cui il Titolare fornisce all'Interessato tutte le informazioni che il GDPR dispone gli vengano date.

L'informativa può contenere, in calce, una parte dedicata ai consensi ed è comunque opportuno farla firmare dall'Interessato, conservando l'originale, in modo da poter dimostrare di averla sottoposta alla sua attenzione.

Deve contenere una serie di informazioni obbligatorie:

- l'identità e i dati di contatto del Titolare del trattamento;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza dei diritti dell'Interessato;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo al Garante della privacy;
- se la comunicazione dei dati personali sia un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un accordo, e se l'Interessato abbia l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati.

OBIETTIVI

La terminologia, anche se ridotta al minimo come in questo caso, è sempre un po' noiosa; tuttavia è indispensabile per capire di cosa stiamo parlando. Ora veniamo alla parte più pratica. Andiamo a vedere quali siano gli obiettivi del GDPR e come

applicarli a organizzazioni come le nostre.

Quando si pensa alla privacy vengono subito in mente concetti come protezione, riservatezza, ecc.

In realtà l'obiettivo del GDPR è duplice: da un lato sicuramente la protezione e la tutela dei dati e quindi dei diritti dell'Interessato; dall'altro però anche un aspetto meno intuitivo, che consiste nella tutela della libera circolazione dei dati stessi.

Applicare il GDPR significa quindi proteggere i dati senza che le operazioni messe in atto per raggiungere lo scopo, possano ostacolare o limitare la loro libera circolazione.

Questa visione è particolarmente importante nelle realtà come le nostre, perché i dati personali che raccogliamo servono senza dubbio a dar seguito alla volontà dell'Interessato, il quale ce li affida perché vuole partecipare alle attività sociali (allenamenti, partite, premiazioni, ecc.). Anche quando pensiamo a dati personali quali le fotografie da pubblicare sul sito web, bisogna evitare di cadere nella tentazione di ometterle a priori così da non rischiare nulla. Alla maggior parte degli atleti fa piacere apparire su un sito web o su Facebook, fotografati in azioni di gioco o durante le premiazioni. Il loro diritto ad apparire rientra in quella libertà di circolazione dei dati che il GDPR tutela. Nostro compito è informarli, raccogliere il loro consenso e combinare il diritto di quanti vogliano apparire con quello di coloro che invece non lo desiderino, compatibilmente con le nostre capacità organizzative.

Le capacità organizzative sono un altro aspetto al quale il GDPR fa riferimento. E non potrebbe essere altrimenti visto che è un regolamento chiamato a disciplinare i trattamenti più disparati, in attività che spaziano dalle società sportive alle multinazionali, nei diversi Paesi dell'Unione. Le operazioni che metteremo in atto per applicare il GDPR, nelle nostre realtà, devono quindi essere proporzionate alle capacità organizzative.

Queste premesse vanno sempre tenute presente: l'applicazione del GDPR è un gioco di equilibri ed è facile sbilanciarsi per effetto della paura delle sanzioni. Ricordiamo però che le sanzioni sono previste perché altrimenti - noi italiani lo sappiamo bene - il GDPR resterebbe lettera morta. Sfruttiamo quindi la paura delle sanzioni per applicare al meglio il GDPR e, così facendo, non avremo nulla da temere.

IL PERCORSO

Gli obiettivi enunciati nel paragrafo precedente, obbligano di fatto il Titolare del trattamento a porre in atto azioni idonee a perseguirli.

In pratica un percorso che possiamo suddividere in cinque fasi:

1. Acquisizione delle informazioni sulle disposizioni del GDPR

2. Analisi di quali siano i trattamenti, con quali mezzi vengano effettuati e quali persone se ne occupino

3. Elaborazione della strategia per il raggiungimento degli obiettivi

4. Messa in pratica della strategia elaborata

5. Controllo della corretta applicazione e aggiustamenti alla strategia

La conformità al GDPR è un processo, non un atto, o una serie di atti, da compiere in un dato momento e poi non pensarci più. Anche in questo, la distanza con la precedente normativa è notevole: non ci viene richiesto di compilare un documento iniziale da aggiornare tutti gli anni (come succedeva con il famoso DPS), quanto piuttosto di creare un sistema interno, da verificare e migliorare costantemente, che ci consenta, ogni qualvolta trattiamo dati personali, di perseguire gli obiettivi prefissati.

Continuando a ragionare da italiani, la pretesa sembra eccessiva e sproporzionata. Ma è proprio questo il punto, ci viene richiesto un upgrade (qui l'esterofilia è molto utile) di mentalità. Cioè dobbiamo acquisire una nuova forma mentis per i dati personali. Nessuno di noi lascerebbe incustodita una banconota da 50 euro, nemmeno sul luogo di lavoro o nella sede della società sportiva. Se una persona lo facesse abitualmente verrebbe considerato dagli altri quantomeno poco affidabile. Al valore dei soldi veniamo addestrati fin da bambini ed è per noi naturale: ci viene richiesto di far diventare altrettanto naturale l'attenzione verso i dati personali altrui.

Per acquisire un nuovo automatismo bisogna esercitarsi e aiutarsi a vicenda. In questo i dirigenti delle società sportive sono agevolati perché sono abituati a collaborare, a migliorarsi e a far progredire gli atleti. Per inserire il GDPR in un questo continuo miglioramento è opportuno dotarsi di alcuni strumenti.

GLI STRUMENTI

La parola strumenti in questo caso significa "mettere per iscritto". A mano o a computer poco importa, bisogna scrivere, anche se da alcuni è ritenuta l'attività più noiosa (e inutile) del mondo. In realtà è utilissima, anche se faticosa: la codifica e la trasmissione delle informazioni, nella maggior parte dei casi avviene grazie alla forma scritta. Fortunatamente non dobbiamo sempre scrivere partendo da zero ma ci possiamo appoggiare a modelli già predisposti.

Come avrai notato, questo vademecum ha un taglio molto pratico, la parte teorica è ridotta all'essenziale. Riprendo dunque i passaggi del paragrafo precedente, a uno a uno, specificando cosa sia opportuno fare e quale documentazione produrre. Naturalmente sono indicazioni da applicare alla propria specifica realtà, aggiungendo o togliendo, a seconda dei casi.

1. Acquisizione delle informazioni sulle disposizioni del GDPR

Queste pagine sono state pensate per fornirti alcune informazioni sul GDPR e il loro possesso testimonia (dimostra) la tua volontà fattiva di acquisizione delle nozioni di base. Leggere il Regolamento vero e proprio ti permette di avere il quadro completo, lo trovi facilmente in Internet (l'articolo 1 è a pagina 38 dopo le infinite considerazioni iniziali).

Per molti leggere è più faticoso che ascoltare, quindi partecipare ad eventi di formazione, dal vivo oppure online, è un'ottima idea. Per dimostrare l'attività svolta è opportuno farsi rilasciare un attestato di partecipazione, da conservare tra i documenti GDPR, e predisporre una scheda nella quale prendere nota di tutte le iniziative formative alle quali qualcuno della società sportiva ha preso parte.

La normativa evolve, ad esempio con i chiarimenti e i provvedimenti del Garante, e le informazioni acquisite possono essere dimenticate, specie se non vengono rinfrescate. È indispensabile programmare periodici approfondimenti in modo da non lasciare la scheda formativa ferma per troppo tempo.

2. Analisi di quali siano i trattamenti, con quali mezzi vengano effettuati e quali persone se ne occupino

In questo caso il primo intervento consiste nel pensare - meglio se insieme ad altri in una riunione - quali siano le attività di trattamento effettuate dalla società sportiva, con quali mezzi siano effettuati e quali persone siano coinvolte, in modo da formulare una strategia per l'applicazione del Regolamento alla propria specifica realtà.

Il GDPR propone uno strumento, il Registro delle attività di trattamento (art. 30), non obbligatorio per le nostre realtà, che risponde, tra le altre cose, all'esigenza di censire i trattamenti in essere.

Per avere sotto controllo il quadro della situazione, e dimostrare di averlo, è opportuno raggruppare in una scheda le informazioni sintetiche relative ai trattamenti, ai mezzi utilizzati, insieme alle misure di sicurezza e alle persone incaricate al trattamento.

È anche opportuno scrivere una sorta di organigramma interno, magari da esporre nella propria sede, in modo che tutti sappiano chi ricopra determinati ruoli ai fini della privacy.

3. Elaborazione della strategia per il raggiungimento degli obiettivi

All'analisi del punto precedente, supportata dalle schede che ci aiutino a tenere sotto controllo i diversi aspetti, segue l'elaborazione della strategia, tagliata su misura per le nostre esigenze e possibilità.

La strategia è il cuore della nostra azione e copre diverse aree di intervento:

a. formazione delle persone interne (incaricati) che trattino i dati personali e predisposizione di supporti informativi (istruzioni pratiche);

b. messa in sicurezza dei luoghi fisici per gli archivi cartacei e dei dispositivi elettronici per quelli digitali;

c. predisposizione di un archivio GDPR che raccolga i moduli destinati all'informazione degli Interessati (le informative), i moduli con la contrattualistica, le procedure interne, ecc.;

d. predisposizione di un archivio contenente i consensi raccolti dagli Interessati e le successive richieste di modifiche agli stessi consensi e ai dati personali.

Tutto ciò può sembrare eccessivo, tuttavia se applicato con la dovuta attenzione e sensibilità, contribuisce a dare quadratura a tutta l'organizzazione e sviluppa fiducia (perché dimostra che il gruppo prende tutte le questioni nella dovuta considerazione).

4. Messa in pratica della strategia elaborata

L'elaborazione della strategia è necessaria ma non sufficiente al raggiungimento degli obiettivi: è indispensabile che venga attuata. Sarà compito del referente individuare le risorse a disposizione e affidare ad esse le mansioni da compiere per applicare la strategia nella pratica. Seguono una serie di suggerimenti di base, per ogni punto della strategia, da integrare in relazione alle caratteristiche della propria società sportiva.

a. formazione delle persone interni (incaricati) che trattino i dati personali e predisposizione di supporti informativi (istruzioni pratiche)

Si tratta di spiegare il GDPR, a voce o con il supporto di materiale scritto (ad es. questo vademecum), alle persone interne preposte al trattamento dei dati personali. Non è possibile affidare mansioni operative interne, che implichino trattamento di dati personali, senza aver opportunamente formato la persona al rispetto del Regolamento. Alle informazioni, verbali o scritte, è sempre meglio aggiungere schemi pensati per la specifica mansione, in modo da aiutare la persona ad assimilare e ricordare nel tempo le procedure. Indispensabile è anche l'azione di feedback periodico, che consiste nel chiedere personalmente, all'incaricato interno, quali difficoltà abbia incontrato nell'applicare in pratica le informazioni sul GDPR che il referente, o chi per lui, gli ha trasmesso.

b. messa in sicurezza dei luoghi fisici per gli archivi cartacei e dei dispositivi elettronici per quelli digitali

In tutte le società sportive andranno probabilmente attuate sia le misure per i luoghi fisici sia quelle per i dispositivi elettronici, perché è sufficiente scrivere o stampare un elenco di dati per ricadere nel primo gruppo e ricevere posta elettronica per rientrare nel secondo.

Per i luoghi fisici è necessario riporre gli archivi cartacei di dati personali in locali ad accesso riservato con armadi o cassetti chiusi a chiave, per evitare che persone non autorizzate (ad es. chi si occupa delle pulizie) possano accedere ai dati stessi. È anche importante impartire, per iscritto, precise istruzioni affinché gli incaricati interni adottino il massimo riserbo, non effettuino copie non autorizzate e mettano in atto una corretta modalità di distruzione dei supporti cartacei una volta venuta meno la loro utilità.

Per quanto riguarda i dispositivi elettronici, che ospitino anche temporaneamente dati personali, è indispensabile siano protetti da password (o altro sistema di accesso sicuro). Inoltre, è necessario che l'opzione per il blocco automatico del dispositivo, dopo pochi minuti di inutilizzo, sia attivata e che venga richiesta la password (o altro sistema di accesso sicuro) per rientrare nel dispositivo. I sistemi operativi devono essere aggiornabili (cioè ancora supportati dalla casa madre) e aggiornati, devono essere dotati di antivirus e i dati personali devono essere salvati periodicamente (backup), ad esempio su un'unità esterna anch'essa crittografata oppure riposta in luogo sicuro (sottochiave).

Per quanto riguarda i dispositivi mobili (ad es. notebook, tablet, smartphone, chiavette USB, ecc.), particolarmente esposti al rischio di furto o smarrimento, si consiglia il ricorso alla crittografia in quanto i sistemi operativi più diffusi (Windows, Android, ecc.) dispongono di funzionalità native a costo zero (ad es. Bitlocker, solo per le versioni PRO di Windows)

oppure di soluzioni gratuite open source (ad es. VeraCrypt). Qualora gli associati utilizzassero dispositivi mobili personali per svolgere mansioni relative alla società sportiva, implicanti il trattamento di dati personali (ad es. memorizzazione di archivi sociali, scaricamento in locale della posta elettronica della società sportiva, ecc.) questi dispositivi, o archivi, andranno crittografati.

Laddove non fosse possibile crittografare il dispositivo mobile, o l'archivio memorizzato su di esso, dovranno essere impartite istruzioni, sempre per iscritto, affinché non vi vengano salvati, neanche temporaneamente, dati personali della società sportiva. È possibile, ad esempio, accedere alla posta elettronica attraverso la pagina web messa a disposizione dal provider (webmail), quindi senza memorizzare nulla in locale, e lavorare su documenti che risiedano su una memoria esterna crittografata (ad es. chiavetta USB, ecc.) oppure su un servizio remoto in cloud attraverso applicativi web (es. Microsoft Office Online). È sempre opportuno gestire la posta elettronica della società sportiva su caselle e-mail dedicate, tenendola separata dalla posta personale.

c. predisposizione di un archivio GDPR che raccolga i moduli destinati all'informazione degli Interessati (le informative), i moduli con la contrattualistica, le procedure interne, ecc.

Mi riferisco alle informative (scaricabili, già predisposte, dal sito web del CTA), alla modulistica in bianco, ad esempio il modello di contratto da sottoporre ai Responsabili del trattamento, privi di dati personali in quanto non compilati, ai documenti informativi e alle procedure interne.

È opportuno riporre tutto ciò che riguarda il GDPR in un fascicolo, in modo che gli incaricati interni possano accedervi facilmente all'occorrenza. La stessa cosa andrà fatta sui dispositivi elettronici, creando una cartella apposita, qualora risultasse più comodo il loro utilizzo in relazione alle abitudini organizzative interne.

d. predisposizione di un archivio contenente i consensi raccolti dagli Interessati e le successive richieste di modifiche agli stessi consensi e ai dati personali

La stessa procedura del punto precedente va messa in atto per i moduli già compilati (ad es. i contratti con i Responsabili del trattamento), quindi contenenti dati personali, e per i consensi raccolti, avendo cura però di riporli sottochiave se in formato cartaceo e protetti da password (e da crittografia per i dispositivi mobili) laddove in formato elettronico.

5. Controllo della corretta applicazione e aggiustamenti alla strategia

Per monitorare l'applicazione della strategia bisogna programmare periodicamente dei momenti di incontro, a due (tra il referente, o chi per lui, e l'incaricato interno) oppure in riunioni con tutto lo staff, nei quali vengano riportate le eventuali difficoltà, i suggerimenti di miglioramento e si possano studiare aggiustamenti alla strategia inizialmente pensata.

È importante che questi momenti di incontro abbiano delle ricadute sul piano documentale, sia con l'aggiornamento delle istruzioni e delle procedure scritte, sia con la verbalizzazione da parte del Consiglio Direttivo delle periodiche modifiche alla procedura GDPR, che testimonino la costante attenzione della società sportiva alla sua effettiva applicazione. A questo proposito è opportuno apporre in calce alla documentazione la dicitura "documento aggiornato il" oppure "revisione documento del" ecc. seguita dalla data dell'ultimo aggiustamento.

CONCLUSIONI

L'applicazione del GDPR richiede senza dubbio il lavoro di squadra dello staff e questo può comportare delle resistenze da parte delle persone coinvolte. È importante sottolineare che, nelle nostre realtà, chi ricopre il ruolo di presidente si accolla già delle importanti responsabilità. Le indicazioni contenute in questo vademecum, se applicate correttamente, consentono di adeguarsi alle disposizioni di legge senza affrontare i considerevoli costi derivanti da consulenze esterne alla società sportiva. Il concorso da parte di tutti alla loro attuazione rappresenta un gesto di sensibilità e solidarietà verso il presidente della società sportiva che altrimenti verrebbe gravato di un rischio ulteriore.

Le procedure suggerite nel documento costituiscono un punto di partenza e il mio auspicio è di perfezionarle strada facendo, anche grazie al confronto con le società sportive che adottino al loro interno soluzioni migliorative. Metteremo a disposizione una pagina web nel sito del CTA dove sarà possibile scaricare la versione sempre aggiornata del vademecum, nonché quei moduli già predisposti (penso all'organigramma interno, al contratto tipo con i Responsabili del trattamento, alle schede interne per controllare i trattamenti, le misure adottate, ecc.) che le società sportive vorranno liberamente condividere.

Materiale e suggerimenti possono essere inviati a privacy@cta.mi.it

ultimo aggiornamento 24/09/2018