LA PROTEZIONE DEI DATI PERSONALI

Il GDPR tra obblighi di adeguamento e sanzioni

Cos'è il GDPR?

Il Regolamento UE 2016/679, anche noto come GDPR (General Data Protection Regulation) ha riformato e armonizzato le legislazioni degli Stati membri dell'UE in materia di trattamento e circolazione dei dati personali.

Quali sono i dati oggetto del trattamento?

Per le associazioni e le società sportive, sono oggetto di trattamento:

- Dati anagrafici (nome, cognome, codice fiscale, data e luogo di nascita, residenza)
- Mail e numero di telefono
- Certificato medico
- Eventuali dati sensibili (razza ed etnia, convinzioni religiose, filosofiche o politiche, orientamento sessuale, situazione sanitaria)

Consenso: cosa cambia rispetto al Dlgs. n. 196/2003

Il consenso deve essere esplicito per i **dati sensibili** e quelli raccolti con **profilazioni** o **trattamenti automatizzati**

Si considera valido il consenso espresso dal minore che abbia compiuto 16 anni

Cosa non cambia

Il consenso deve essere:

- Libero
- Specifico
- Informato
- Inequivocabile

La manifestazione del consenso deve avvenire mediante dichiarazione o azione positiva inequivocabile.

Non è ammesso il consenso tacito o presunto

Adeguarsi alla nuova normativa

Il Regolamento UE 2016/679 pone l'accento sulla **responsabilizzazione** (accountability) di titolari e responsabili al trattamento.

Le misure proattive che assicurano l'applicazione della nuova normativa sono:

- L'indicazione e nomina dei responsabili e incaricati al trattamento
- La redazione di un Registro dei trattamenti
- L'analisi dei rischi e la valutazione d'impatto sulla protezione dei dati
- L'adozione di misure di sicurezza idonee
- L'adeguamento dell'informativa e delle prassi relative all'esercizio dei diritti da parte degli interessati
- La notificazione di eventuali violazioni

Il Registro dei trattamenti

Da redigere in forma scritta (anche elettronica), racchiude l'insieme delle **operazioni di trattamento.**

N.B. *INSIEME ALL'INFORMATIVA E' IL DOCUMENTO FONDAMENTALE DA ESIBIRE ALL'AUTORITA' DI CONTROLLO IN CASO DI ISPEZIONE*

Analisi dei rischi e valutazione d'impatto sulla protezione dei dati

In base alle modalità con le quali avviene il trattamento (si dovrà tenere conto del perché i dati vengono raccolti, conservati, eventualmente trasmessi o distrutti) dovranno essere identificati eventuali **rischi rilevanti**.

Fatto ciò, sarà necessario compiere una valutazione dell'impatto che i rischi hanno sul trattamento.

La **valutazione d'impatto** o **DPIA** (Data Protection Impact Assessment) potrà essere compiuta anche attraverso software (es. PIA).

Alla luce dei rischi e dell'impatto, l'organizzazione sarà tenuta a prendere delle misure protettive idonee.

Misure di sicurezza

Non esistono obblighi generalizzati per l'adozione di misure minime di sicurezza.

L'organizzazione deve tenere conto della DPIA per identificare buone prassi o strumenti per tutelare i dati. In tal senso può essere utile anche aderire ad un codice di condotta.

L’informativa sulla privacy

La nuova normativa deve citare i riferimenti normativi nazionali ed europei (Dlgs. 196/2003 e ss. modifiche, Reg. UE 2016/679).

Contenuti:

- Anangrafica e indirizzo della sede legale dell’Entità giuridica
- Titolare del trattamento e rappresentante legale
- Base giuridica e finalità del trattamento
- Eventuale trasferimento di dati a terzi (es. EPS, FSN o CONI)
- Periodo di conservazione dei dati
- Eventuali processi automatizzati (es. software gestionali, profilazioni ecc.)
- Diritti degli interessati

Tempi:

L’informativa deve essere data in visione prima della raccolta dei dati.

Nel caso la raccolta non avvenga direttamente presso l’interessato l’informativa deve essere fornita entro un mese.

L’esercizio dei diritti da parte degli interessati

Il titolare del trattamento deve assicurare agli interessati la fruibilità dei seguenti diritti sui dati comunicati:

- Diritto di accesso
- Diritto di cancellazione (diritto all’oblio)
- Diritto a limitare il trattamento

La notifica delle violazioni

In caso di violazione dei dati personali, tutti i titolari del trattamento sono tenuti a documentare, indicando circostanze, modalità e gravità degli accadimenti.

Se dalla violazione derivino rischi per gli interessati, l'organizzazione sarà tenuta entro 72 ore a notificare quanto avvenuto all'Autorità Garante per la Protezione dei Dati Personali.

Normalmente quanto descritto è documentato con la compilazione di un modulo di Data Breach.

Le sanzioni

A seconda della tipologia di violazione (quando compiuta direttamente da titolare del trattamento o anche ad esempio per *culpa in vigilando*) possono essere comminate diverse tipologie di sanzioni.

Penali: non si tiene conto solo del profitto derivante eventualmente dall'illecito ma anche del danno arrecato all'immagine o reputazione della vittima

Correttive: quando una violazione della normativa sia di limitata entità, l'Autorità di controllo può decidere di rivolgere ammonimenti o ingiungere di adottare determinati comportamenti.

Amministrative: Ai fini dissuasivi, l'Autorità di controllo può decidere di comminare sanzioni amministrative pecuniarie, parametrate su:

- Natura, gravità e durata della violazione
- Presenza di dolo o colpa
- Categoria di dati interessata dalla violazione
- Misure adottate per analizzare il rischio, valutarne l'impatto ed eventualmente limitarne il danno.