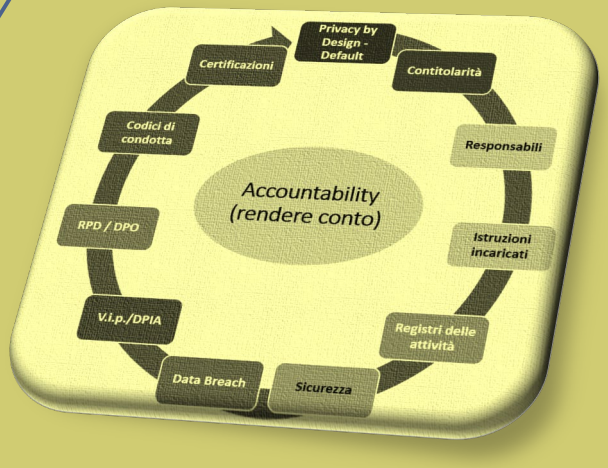
GDPR (General Data Protection Regulation)
(Regolamento Generale sulla Protezione dei Dati)

NELLO SPORT

APPROCCIO ATTIVO SULLE TUTELE DEI DATI PERSONALI



CON IL PRINCIPIO DI ACCOUNTABILITY

IL GDPR INDICA AL TITOLARE E AL RESPONSABILE DEL TRATTAMENTO LO SCOPO DA RAGGIUNGERE (LA GARANZIA DELLA TUTELA E PROTEZIONE EFFETTIVA DEI DATI PERSONALI), RIMETTE, ALLA LORO RESPONSABILITÀ INDIVIDUALE, L'INDIVIDUAZIONE DELLE MISURE ADEGUATE DA ADOTTARE NELL'AMBITO DI UN VERO PROGRAMMA DI PROTEZIONE DEI DATI.

BY DESIGN

DELLE MODALITÀ DI TRATTAMENTO DEI DATI, IL TITOLARE ED IL RESPONSABILE DEL TRATTAMENTO DOVRANNO VALUTARE LA NATURA DELLE ATTIVITÀ DI TRATTAMENTO CHE PONGONO IN ESSERE ED I RISCHI CHE TALI ATTIVITÀ POSSONO COMPORTARE.

BY DEFAULT

TUTTE LE MISURE NECESSARIE A GARANTIRE UNA EFFETTIVA E ADEGUATA PROTEZIONE DEI DATI PERSONALI

ADOTTARE UN MODELLO PRIVACY "SU MISURA" IN MODO DA RIDURRE I RISCHI SUI DIRITTI E SULLA LIBERTÀ DELLA PERSONA

I DIRITTI DELL'INTERESSATO

- Rettifica
- Cancellazione
- Limitazione al trattamento
- Trasferimento ad un altro titolare (diritto alla portabilità)
- Ottenere copia
- Essere informato

COSA SI INTENDE PER DATO PERSONALE?

Qualsiasi informazione che identifica, direttamente o indirettamente, una PERSONA FISICA.

CHI DEVE ADEGUARSI?

Chiunque effettui un trattamento dati (raccolta, archiviazione, comunicazione, modifica, cancellazione) che ecceda un uso personale o domestico.

QUALI DATI SONO "PARTICOLARI"?

Quelli che rivelano origine razziale o etnica, convinzioni religiose, filosofiche, opinioni politiche, appartenenza sindacale o relativi alla salute, alla vita sessuale; oltre a dati genetici, dati biometrici e relativi all'orientamento sessuale, introdotti dal GDPR.

CRITERI PER APPLICAZIONE DELLE SANZIONI

- Natura e gravità della violazione
- Dolo o colpa
- Misure tecniche e organizzative adottate
- Precedenti violazioni
- Grado di cooperazione
- Rispetto di un precedente provvedimento
- Adesione a codici di condotta

GRUPPI

Primo gruppo di sanzioni e le violazioni degli obblighi imposti ai seguenti soggetti:

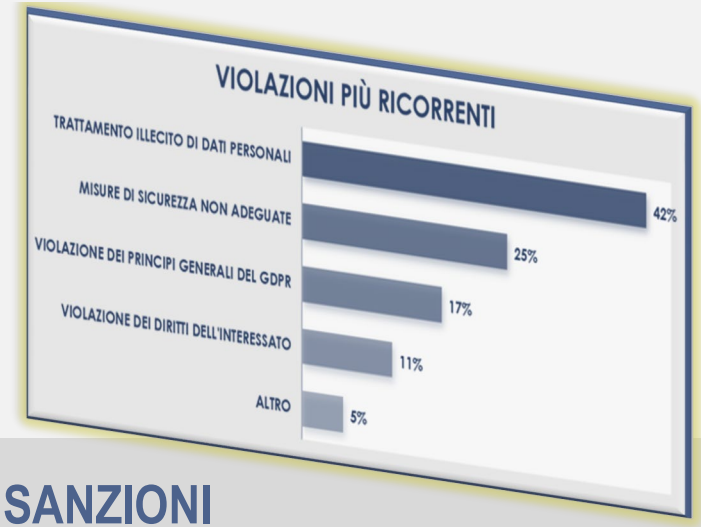
- il titolare ed il responsabile del trattamento (art. 8, 11, da 25 a 39, 42 e 43 GDPR);
- l'organismo di certificazione (esempio Accredia);
- l'organismo di controllo dei codici di condotta (art. 41 GDPR);

Il secondo gruppo di sanzioni, più pesanti in considerazione della maggiore gravità delle fattispecie a cui sono ricondotte, riguardano nello specifico le seguenti violazioni:

- 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;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
- qualsiasi obbligo ai sensi delle legislazioni degli Stati, paragrafo 2, o il negato accesso in violazione dell'articolo 58, membri adottate a norma del capo IX;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo (ovvero il Garante Privacy) ai sensi dell'articolo 58.

I PRINCIPI CARDINI DA RISPETTARE

- Liceità, correttezza e trasparenza
- Proporzionalità e necessità
- Minimizzazione dei dati
- Esattezza dei dati
- Sicurezza adeguata



SANZIONI

PENALI

- Trattamento illecito
- Comunicazione, diffusione e acquisizione fraudolenta
- False dichiarazioni o inosservanza di provvedimenti

(ART. 167-171 GDPR)

AMMINISTRATIVE

SANZIONI PECUNIARIE ART.83-84 GDPR

LA VALUTAZIONE DI IMPATTO DEI RISCHI
(ART. 35 GDPR)

Si tratta di un processo di valutazione della conformità alle norme, valutando il "rischio di impatti negativi sulle libertà e i diritti degli interessati".

È OBBLIGATORIA?

Sì, per trattamenti a "rischio elevato", come nel caso delle SSD e ASD, che trattano in modo non occasionale dati particolari anche di soggetti vulnerabili (minori e disabili).

INFORMATIVA

Il contenuto dell'INFORMATIVA deve essere CHIARO e SEMPLICE (Art. 13 e 14 GDPR).

- **Titolare del trattamento** (SSD o ASD);
- **Interessati** (atleti, tesserati, associati, collaboratori, ecc.);
- **Responsabili del trattamento** (anche esterni come commercialisti, consulenti del lavoro, amministratori di sistema, ecc.);
- **Eventuale nomina DPO** (Data Protection Officer);
- **Finalità del trattamento** (tesseramento, adempimenti di legge, infortuni, procedimenti, giustizia sportiva, ecc.);
- **Base giuridica** (contratto, obblighi di legge, legittimo interesse e consenso);
- **Categorie di dati** (comuni, sanitari, biometrici, ecc.);
- **Destinatari** (Coni, federazioni, consulenti, giornalisti, ecc.);
- **Periodo di conservazione** (10 anni per la tutela dei diritti);
- **Possibilità di reclamo al Garante.**

IL CONSENSO (ART. 4 GDPR)

Il consenso è necessario quando non c'è una valida base giuridica.

Per essere validamente espresso deve esserci una "dichiarazione o azione positiva inequivocabile".

IL CONSENSO DEVE ESSERE:

- Espresso liberamente
- Specifico
- Informato
- Prestato per ogni finalità di trattamento
- Sempre revocabile

IL REGISTRO DEI TRATTAMENTI (ART 30 GDPR)

È un documento che contiene le principali informazioni sulle categorie dei trattamenti, non sui singoli interessati.

È OBBLIGATORIO NELLO SPORT?

Il Garante della Privacy (comunicato 8 ottobre 2018) ha precisato che è obbligatoria per le "associazioni sportive con riferimento ai dati sanitari trattati". In ogni caso è lo strumento principale per il rispetto del principio di accountability, per cui è sempre consigliabile.

DOMANDE PIÙ COMUNI

SSD E ASD SONO TITOLARI DEI DATI RACCOLTI PER IL TESSERAMENTO PRESSO LE FEDERAZIONI?

- No, sono RESPONSABILI DEL TRATTAMENTO perché raccolgono dati per conto delle federazioni;
- Sono TITOLARI dei dati per altri trattamenti (corsi, ritiri, ecc.).

È OBBLIGATORIA LA NOMINA DEL DPO?

Il Data Protection Officer è una figura di controllo indipendente, obbligatoria solo per enti pubblici e soggetti che effettuano un monitoraggio sistematico e/o trattamento di dati particolari su larga scala (es. le federazioni).

QUALI DATI PARTICOLARI VENGONO TRATTATI NELLO SPORT?

- Sanitari (patologie, infortuni e intolleranze);
- Biometrici (performance, impronte e riconoscimento facciale);
- Religione o razza (alimentazione o attività in particolari periodi);

IL CERTIFICATO DI IDONEITÀ SPORTIVA CONTIENE DATI PARTICOLARI?

Il certificato di idoneità non contiene dati particolari se non rivela particolari inidoneità, patologie o dati biometrici.

OBBLIGO DI DATA BREACH (Art. 33-34 GDPR)

Lo scopo è quello, in caso di violazione, di permettere all'Autorità di controllo di attivarsi senza ritardo in modo da valutare la gravità della violazione e la tipologia di misure da imporre al Titolare:

- Natura della violazione
- Natura dei dati
- Numero di interessati
- Nome e contatto del Resp. o di altro referente
- Descrizione delle probabili conseguenze

RESPONSABILE → TITOLARE → AUTORITÀ DI CONTROLLO

Comunicare il Data Breach entro le 72 ore.

ASPETTI DELLA TUTELA DELL' IMMAGINE

- Sfruttamento economico dell'immagine
- Protezione contro gli abusi.

NB.: Si può trasferire il diritto allo sfruttamento economico dell'immagine, non il diritto all'immagine costituzionalmente garantito.

LE NORME

ART. 96 e 97 (Legge Diritto d'Autore n. 633/1941)

L'immagine altrui può essere utilizzata:

1) quando c'è il consenso della persona interessata

2) quando ricorre una causa di giustificazione.

ART. 10 cod. civ.
Qualora l'immagine è esposta o pubblicata fuori dai casi consentiti dalla legge, ovvero con pregiudizio al decoro, l'Autorità Giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso ed il risarcimento del danno.

CONFINI DELL' IMMAGINE IN EVENTI PUBBLICI

Non si configura lesione del diritto alla privacy del soggetto che durante un servizio televisivo viene ripreso mentre si trova nel luogo di partenza di molti manifestanti.
L'esposizione o la pubblicazione dell'immagine altrui non può infatti considerarsi abusiva quando si ricolleghi a fatti di interesse pubblico o svoltisi in pubblico, dovendosi ritenere compresi quegli episodi che, pur non integrando in sé l'evento, al medesimo si ricolleghino in modo inequivocabile.

CAUSE DI GIUSTIFICAZIONE

Ricorre una causa di giustificazione e non serve quindi il consenso quando… Art. 97 LDA

L'uso dell'immagine è giustificata da:

- Notorietà o dall'ufficio pubblico ricoperto
- Necessità di giustizia o di polizia
- Da scopi scientifici, didattici o culturali
- Riproduzione collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico.

La causa di giustificazione deve essere reale ed effettiva e avendo carattere derogatorio della disciplina al diritto all'immagine costituzionalmente garantito, non è ammessa applicazione estensiva.

La causa di giustificazione ricorre effettivamente se l'immagine o la notizia riguarda un soggetto con elevato grado di notorietà:

- Se contribuisce ad un dibattito di interesse pubblico;
- Se c'è un interesse effettivo ed attuale alla sua diffusione;
- Se la notizia è veritiera e diffusa a soli fini informativi, dandone preventiva comunicazione all'interessato per la replica.

COPYLEFT

Una licenza Copyleft è definita da due aspetti principali:

- La libertà per gli utenti di modificare e distribuire opere derivate;
- La clausola "share-alike" che mantiene la libertà nei lavori derivati.

Le licenze Copyleft esistono all'interno della struttura legale dei diritti d'autore e non riguardano l'abolizione dei diritti d'autore, ma sono un sottoinsieme delle licenze di copyright con l'obiettivo di ripristinare la libertà degli utenti.

LESIONE DELL'IMMAGINE

La pubblicazione di un video su Youtube, ove gli utenti possono visionare e condividere il video, rientra nella disciplina europea di trattamento dei dati personali.

Spetta al Giudice però valutare se una tale diffusione possa avere scopo divulgativo di informazioni al pubblico o costituisca una violazione del trattamento dei dati personali.

FOTOGRAFIE SUI SOCIAL NETWORK

Ex art. 700 cpc

- L'inserimento di fotografie nelle pagine social network equivale a pubblicazione;
- Non rileva che la visibilità sia ristretta solo ai follower/amici;
- Costituisce attività in sé pregiudizievole, poiché consente la diffusione dei dati ad alta rapidità e rende inefficaci le misure ex post;
- È quindi applicabile il provvedimento d'urgenza, specialmente quando riguarda minorenni.

In caso di abuso dell'immagine, l'interessato o uno degli stretti congiunti sopra elencati - potrà ottenere dal giudice l'ordine inibitorio di cessazione dell'abuso, oltre al risarcimento dei danni patrimoniali (v. 2043) e non patrimoniali (v. 2059) subiti.

L'autore di pubblicazioni illecite di foto e/o filmati offensivi della reputazione di chi vi è ritratto, dovrà non solo risarcire il danno ma rispondere anche del reato di diffamazione aggravata (art. 595 cod. pen.).

DA e-PD A e-PR (e-PRIVACY Regulation)

La direttiva ePD (ePrivacy Directive) sarà presto trasformata in un regolamento e sarà sempre più complementare al GDPR, permettendo di rafforzare la sfera privata dei cittadini online e regolare più intensivamente la protezione dei dati. Tuttavia, mentre il GDPR mira in generale ad assicurare la protezione dei dati personali, il Regolamento ePrivacy mira ad assicurare la riservatezza, la sicurezza delle comunicazioni elettroniche e l'integrità delle informazioni contenute nei dispositivi elettronici utilizzati per comunicare (quali smartphone, tablet, ecc.), che contengano o meno dati personali.

La proposta di regolamento su "ePrivacy" richiama espressamente le definizioni stabilite dai seguenti testi normativi:

- GDPR;
- Direttiva (UE) 2018/1972 dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche;
- Direttiva 2008/63/CE della Commissione del 20 giugno 2008 relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazione;
- 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 (codificazione).

SERVIZI DI COMUNICAZIONE OVER-THE-TOP ("OTT")

- Rete di comunicazione elettronica
- Servizio di comunicazione elettronico
- Servizio di comunicazione interpersonale
- Servizio di comunicazione interpersonale basato sul numero
- Servizio di comunicazione interpersonale indipendente dal numero

AMBITO DI APPLICAZIONI

Una delle principali novità della Direttiva ePrivacy è l'estensione del campo di applicazione ai cosiddetti fornitori di servizi over-the-top ("OTT") come WhatsApp, Facebook, Messenger e Skype, ossia i fornitori di servizi di comunicazione basati sull'uso della rete Internet, come i servizi di instant messaging. Pertanto i fornitori OTT saranno tenuti al rispetto delle regole e a garantire lo stesso livello di tutele dei "tradizionali" operatori di telecomunicazione.

METADATI

Il ePR copre i metadati delle comunicazioni elettroniche ("i dati trattati in una rete di comunicazione elettronica per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche compresi i dati usati per tracciare e identificare la fonte e il destinatario di una comunicazione, i dati relativi alla localizzazione del dispositivo generati nel contesto della fornitura di servizi di comunicazione elettronica nonché la data, l'ora, la durata e il tipo di comunicazione ") e il loro contenuto nella trasmissione. Se il trattamento dei metadati è necessario ai fini della fatturazione, i metadati pertinenti possono essere conservati fino alla fine del periodo durante il quale una fattura può essere legalmente contestata o un pagamento può essere preteso..

IOT

Viene menzionata la specificità "dell´internet degli oggetti" al fine di estendere il principio di confidenzialità delle comunicazioni anche ai trattamenti machine-to-machine, ovvero al mondo degli oggetti e dei luoghi concreti

MARKETING DIRETTO

Le comunicazioni di commercializzazione diretta (marketing diretto) - ovvero "qualsiasi forma di pubblicità, scritta od orale, inviata a uno o più utenti finali identificati o identificabili di servizi di comunicazione elettronica, anche mediante sistemi automatici di chiamata e comunicazione con o senza interazione umana, email, SMS, ecc..." richiederanno il consenso degli utenti finali. Inoltre, se gli utenti finali hanno acconsentito a ricevere comunicazioni di marketing diretto, dovrebbero essere in grado di recedere facilmente da tale consenso in qualsiasi momento.

CONSENSO PER L'USO DEI COOKIE ATTRAVERSO IMPOSTAZIONI DEL BROWSER

Un altro elemento innovativo riguarda i cookie. Per rimediare all'eccesso di "cookie banner" che si presentato quotidianamente agli utenti di Internet, si consentirà agli utenti di gestire il proprio consenso ai "cookie di terze parti" tramite le impostazioni del browser. L´utente potrà compiere una scelta unica, accettando o rifiutando in blocco l´installazione dei cookie tramite un settaggio preliminare del browser. Il consenso non sarà invece necessario per l´installazione dei cookie cd. analytics, quelli utilizzati ad esempio per contare gli utenti che visitano uno specifico sito web o per tener traccia degli acquisti nel proprio carrello elettronico.

INFORMATIVA E ACQUISIZIONE DEL CONSENSO

Dovranno essere maggiormente user friendly anche mediante l'impiego di icone stardardizzate.