

Annual Sports Conference 2026: technology, data and AI

Speakers: Christian Scotland-Williamson; Owen O'Rorke; Alan Baker; and David Morgan

Core principles

There is growing regulatory change across Europe (GDPR, privacy rules), increasing sophistication of artificial intelligence (AI) and data-driven technologies, and heightened awareness of how athlete data is collected, processed and commercialised.

This session explored these themes from both athlete and legal perspectives.

Wearable technology and athlete experience

The panel discussed experiences of the use of performance related personal data in English rugby vs the NFL.

- Performance data in the US was often managed **by the athlete** and not monitored by the team, whereas rugby operated a more comprehensive **full athlete profile**, including recovery indicators.
- The use of smart mouthguards:
 - has detected **concussions** in training that would otherwise have been missed;
 - is now being integrated into combat sports where other wearables (eg wrist straps) are not allowed and is growing in use for **scoring**, not just safety.
- However, athlete awareness is low – contractual terms often waive rights without clarity:
 - Example: finding his likeness used in a rugby game without prior knowledge, although players in Madden (NFL) are compensated.

Key compliance considerations

When deploying wearables or AI-driven tech:

- **Accountability** – organisations must demonstrate lawful bases, governance, and oversight.
- **Data Protection Impact Assessments** – essential where data is sensitive or commercialised.
- **Transparency** – athletes must be informed of what data is collected and how it is used.
- **Consent**. Where relying on consent then there it needs to be sufficiently informed.

Under 18s and safeguarding

- Legally, UK GDPR principles don't drastically change – children's rights and parental rights operate under the same framework.
- But **ethical and reputational stakes are much higher**.
- Issues include:
 - enforceability of parental consents;
 - enhanced protections for under 18s; and
 - tension between parental expectations and the child's autonomy.
- Wearables require a **purpose-based justification**:
 - Health protection/injury prevention is easier to justify.
 - Performance measurement is far more nuanced.
- Key question: how much data is being collected on minors, and why?

Privacy, reputation and the attention economy

- Modern sports operate in an **attention economy**.
- Moments of emotional vulnerability can cause reputational and psychological harm when shared publicly.
- Outside the US, athletes increasingly push for **greater control** over personal narrative and data visibility.
- Concern: erosion of 'safe spaces' – athletes perform under total visibility, blurring boundaries between professional and private realms.
- Challenge ahead: balancing fan access with athlete wellbeing.

Project Red Card and athlete data monetisation

- Initiative challenging uncontrolled commercial use of player data.
- Targeted data aggregators – not clubs – based on privacy and data rights.
- Limited success in courts so far, but many claims were handled pre-action.
- Data ownership raises major questions for IP and data lawyers:
 - What categories of sports data can be collected?
 - Who can sell it?
 - Is it personal data, IP, or both?

Personality rights, digital twins and biometric data

- UK GDPR is grounded in human rights, but practically functions 'like a law of personality rights'.
- Digital twins enable:
 - commercial use of athlete likeness; and
 - biometric mapping for gaming, broadcasting, advertising.
- Legal uncertainty:
 - Original image rights frameworks don't fit new realities.
 - How will the law adapt to AI-generated identities?

Athlete awareness and contractual control

- Athletes are often unaware of the extent of data capture and commercialisation.
- Contracts are typically broad, permitting uses that athletes may not fully understand.
- Imbalance of bargaining power:
 - Raising objections can be career-limiting.
 - Athletes rarely challenge terms due to competitiveness and job security concerns.

Fan engagement, marketing and globalisation

- The US works on a **centralised franchise model**.
- Can create tensions:
 - increased travel and marketing duties;
 - increased injury risk and fatigue; and
 - limited ability for athletes to refuse participation.

Website rules, cookies, and marketing compliance

- Regulations are increasingly **rules-based**, with strict enforcement.
- Core areas:
 - cookie consent;
 - privacy notices;
 - preference centres; and
 - direct marketing rules.

- Belief that direct marketing rules are widely misunderstood – organisations are often non-compliant without realising.

Online Safety Act and platform accountability

- Although clubs/athletes are not direct targets, the Act:
 - influences third-party content and due diligence; and
 - requires assessing who you work with and how their platforms engage users.
- Bigger picture:
 - Social media age restrictions (eg TikTok) reshape how athletes connect with fans.
 - May drive **bespoke, self-regulated athlete-fan platforms**.
 - Clubs should conduct broad **risk and impact assessments**, even when not legally required, to show responsible governance.

Discussion points and questions

Female athlete data and menstrual cycle tracking

- Particular sensitivities around tracking in jurisdictions with reproductive laws.
- Data requires robust safeguarding and clear purpose limitation.

Who owns athlete data?

- Legally, personal data belongs to the individual.
- Commercially, data rapidly intertwines with **IP**, creating complex hybrid rights.
- Clinically overseen data adds another layer:
 - Employers often exert ultimate control.
 - Policies must clearly define when data can be shared and by whom.
 - Legal responsibility rests with the organisation, not solely medical staff.

This publication is a general summary of the law. It should not replace legal advice tailored to your specific circumstances.

© Farrer & Co LLP, March 2026