PRIVACY NOTICE

PlayerData Limited and PlayerData Inc.

1. Introduction

PlayerData Limited (registered in Scotland, SC571960) and PlayerData Inc. (a Delaware corporation) (together "**PlayerData**", "**we**", "**us**", "**our**") are committed to protecting personal data.

This Notice explains how we collect and use personal data through:

- our website (www.playerdata.com) and the PlayerData app
- EDGE devices and other PlayerData equipment, including all video cameras (together, the "**Equipment**")
- the provision of processing and analysis of video recorded through the video camera Equipment (the "**Video Analysis Services**")

in each case as updated, enhanced or replaced by PlayerData from time to time (together, the "**Services**").

2. Our Role: Controller or Processor

How we handle your personal data depends on how you interact with us. This affects who you should contact if you have questions about your data.

When we act as a data processor

PlayerData provides its Services to sports clubs and entities, teams, educational institutions and other similar organisations ("**Customers**"). Where a Customer uses our Services to collect and analyse performance and video data about athletes and other users ("**Authorised Users**"), the Customer is the data controller of that data. PlayerData processes it only on the Customer's documented instructions, under the data processing terms attached to or included within our Terms of Service ("**DPA**").

If you are an Authorised User of a Customer's account — typically an athlete, coach or team member — your primary contact for questions about your personal data is the organisation that is our Customer (usually your club, team or organisation that you are affiliated to). We are not responsible for the Customer's own privacy practices.

When we act as a data controller

We are the data controller when we collect and use personal data for our own purposes, including:

- operating and improving our website and Services;
- processing orders placed directly with us by individuals for personal use of the Services;
- managing our relationships with Customer contacts (e.g. team managers and administrators);
- direct marketing (where consented or otherwise permitted);
- creating anonymised data, and derived insights, for our own purposes, including: product development (including training our AI systems), analytics, benchmarking, research, and the production of educational, scientific and marketing materials (such as reports, case studies and white papers), which we may publish or otherwise make available, including through our website and resource hub; and

- developing and improving our products, features and AI systems using video content and its associated data, unless the Customer has opted out.

The Services may from time to time include features that PlayerData operates as data controller, including a "**Leaderboard**" (which displays selected performance data of Authorised Users) and the "**Recruitment Platform**" (which makes Authorised Users' profiles, including performance data and video, visible to registered scouts) (together, "**Data Sharing Features**"). Where an Authorised User is enrolled in a Data Sharing Feature, whether by submitting a request through the PlayerData app, or by the Customer enrolling that Authorised User on the basis that the Customer has the necessary consent or other lawful basis, PlayerData processes the relevant personal data as controller for the purpose of operating that feature. The Customer may at any time disable any or all Data Sharing Features for its Authorised Users.

3. What We Collect

From Customers and their contacts (where we are controller)

- Name, job title, email address, phone number, organisation details
- Billing and payment information
- Communications with us

From Authorised Users and the Customer via the PlayerData app and Equipment (where we are processor on behalf of Customer)

- Identification data: first name, last name, date of birth, photo (optional), gender (optional), role (athlete/staff).
- Contact details: email address and phone number
- Technical and device data: IP address, device identifiers, app usage log
- Performance and activity data: distance covered, speed and top speed, sprints, accelerations, decelerations, workload metrics, training load and session intensity, progression and performance history
- Location data: Real time and historical GPS or LPS location during training/matches, movement patterns and positional data
- Video content: where a Customer uses PlayerData video cameras and Video Analysis Services, video footage recorded during training sessions or matches, together with any associated GPS performance overlays
- Where provided by the Customer: height and weight, and heart rate data (see below in respect of heart rate data)

From website visitors

- Technical data: IP address, browser type, cookie identifiers (see Section 10)

Heart Rate and Special Category Data

Heart rate data is health data and is subject to additional protections under applicable data protection laws. PlayerData only processes heart rate data as a processor acting on Customer instructions, including to anonymise it. Customer must confirm that it holds a valid basis under applicable law to instruct such processing. PlayerData does not use heart rate data for its own purposes, except in anonymised form.

Where a Customer and its Authorised Users use third-party heart rate monitoring equipment, PlayerData accepts no liability for the accuracy or security of data generated by equipment it did not supply.

Video Analysis Services

Where a Customer uses our Video Analysis Services, we use computer vision and artificial intelligence to analyse the video footage, for example, to detect the position of players on the pitch and to overlay GPS and performance data onto the video. We do not use facial recognition, and we do not use the video to identify individuals or to create biometric identifiers. Players are linked to their own data through the GPS units they wear, not through their appearance in the footage. Our analysis of video and performance data is automated and is not used to make decisions that produce legal or similarly significant effects on you.

Video recorded by our Customers may also capture others present — opposing players, match officials and members of the public near the pitch. We do not use facial recognition or seek to identify them, and they are not linked to any account. The Customer is the controller of this footage; PlayerData is a controller only where it uses footage for its own purposes, such as improving its products and systems. The relevant controller's legal basis is legitimate interests in recording and analysing sporting activity, balanced against the rights of those captured; anyone affected may object or exercise their rights at dataprotection@playerdata.com (referred to the Customer where it is the controller).

4. Legal Basis for Processing (UK and European Users)

Where we act as controller and you are located in the UK, European Economic Area or Switzerland, our legal bases for processing are:

- Contract: to process orders, deliver Services, and manage Customer relationships.
- Legitimate interests:
  (1) to maintain business records, respond to enquiries, protect our legal rights, operate, secure, support and improve our Services using technical and usage data, and to analyse performance and usage data in order to create anonymised datasets, insights and educational, scientific and marketing materials, in each case where our interests are not overridden by your rights.
  (2) to develop and improve our products, features and AI systems using video content and its associated data collected through the Video Analysis Services, unless the Customer has opted out of such use under their agreement with us, in each case where our interests are not overridden by your rights. You may object to this processing at any time (see section 13 below).
- Legal obligation: to comply with applicable law (e.g. tax, accounting, regulatory requirements).
- Consent:
  (1) for direct marketing and certain cookies. You may withdraw consent at any time by contacting us.
  (2) For Data Sharing Features, our lawful basis is the consent of the Authorised User, given by submitting an in-app request to be enrolled. Where the Customer has enrolled an Authorised User, we rely on the consent or other lawful basis the Customer has confirmed it holds in respect of that Authorised User. You can withdraw your consent at any time by contacting PlayerData support or using an in-app removal option (where available).

Where we act as processor, we process personal data on the Customer's instructions under our DPA.

5. How We Use Personal Data

As controller

- Fulfilling orders and delivering the Services.
- Managing Customer accounts and providing administrative support.
- Billing and invoicing.
- Communicating with Customers and responding to enquiries.
- Direct marketing to Customers and prospects (where consented or permitted under legitimate interests). You can unsubscribe from our promotional emails via the link provided in the emails. Even if you opt out of receiving promotional email messages from us, you will continue to receive administrative messages from us.
- We process performance data in order to create anonymised datasets and insights — for purposes including product development (including training our AI systems), benchmarking, research and analytics, and the production of educational, scientific and marketing materials such as reports, case studies and white papers. We do not identify any individual Authorised User in these materials and we keep anonymised data in that form and do not attempt to re-identify it.
- Using information about how the Services are used (such as app usage logs and technical and device data) to operate, secure, support and improve the Services, including product analytics.
- Developing and improving our products, features, and AI systems using video content collected through our camera equipment and its associated data, unless the Customer has opted out under their agreement with us. We identify under-13s from the information the Customer provides (including date of birth) and do not use their video for this purpose. In this context PlayerData acts as an independent data controller. This processing is carried out in accordance with applicable law. You can object to this use, or ask to opt out, at any time (see section 13 below).
- Complying with legal obligations and enforcing our agreements.

As processor (on Customer instructions only)

- Providing the Services, including generating and displaying performance metrics and video analysis.
- Storing and making performance data and video available to the Customer and its Authorised Users.
- Providing technical support relating to the Services (including supporting Authorised Users with analytics and understanding the Services data).

Data Sharing Features

The Data Sharing Features (**see When we act as a data controller** in Section 2 above) are features that PlayerData operates as data controller. Authorised Users may be enrolled either by submitting an in-app request, or by the Customer enrolling them with the necessary consent or other lawful basis. Where you are enrolled:

- We process identification data (name, club, role) and performance and activity data (such as GPS-derived performance metrics), and for the Recruitment Platform, video in which you appear. Heart rate data is not used in Data Sharing Features.
- Leaderboard entries are visible to other PlayerData Authorised Users.
- Recruitment Platform profiles, including video, are visible to scouts approved by PlayerData. Scouts may export profile data from the Recruitment Platform and share it with colleges, professional teams or other recruiting organisations. PlayerData does not control what scouts do with profile data after export. If you withdraw your enrolment,

we will remove your profile from the Recruitment Platform, but we cannot retrieve or delete profile data that scouts have already exported.

- Entries are retained while you remain enrolled and are removed when you withdraw, when your Customer instructs PlayerData to remove you, or when your account becomes inactive.
- You may withdraw your consent at any time using the in-app removal option. Your Customer may also disable these features for you.
- Where you are under 18, enrolment on the Recruitment Platform requires verifiable parental consent (see Section 12).

6. Sharing Your Information

We share personal data only in the following circumstances:

- Service providers: third parties who help us operate our Services, acting as our processors and bound by appropriate data processing terms. These include cloud hosting providers, CRM, billing, product analytics, communications and monitoring. A current list of processors is available on our trust centre at https://trust.playerdata.com.
- Analytics Partners: We use analytics services such as Google Analytics, Firebase Analytics and Grafana Labs, to collect and process certain analytics data. You can learn more about Google's practices by visiting Privacy Policy – Privacy & Terms – Google, and opt out of them by downloading the Google Analytics opt-out browser add-on, available at Google Analytics Opt-out Browser Add-on Download Page
  Grafana Privacy Policy is found at: Grafana Labs Privacy Policy | Grafana Labs.
- Advertising Partners: On our website, and only where you have accepted advertising cookies, we work with third-party advertising partners (such as Meta) who collect information about your visit to show you ads that may interest you. Our website is intended for organisations and adults. We do not share information from the PlayerData App or Services with advertising partners, and we do not knowingly use advertising cookies in relation to children. You can withdraw your consent at any time through the cookie settings link in our website footer. Some of our advertising partners are members of the Network Advertising Initiative (https://thenai.org/how-to-opt-out/) or the Digital Advertising Alliance (https://optout.aboutads.info), whose opt-out pages explain how to opt out of personalised ads from member companies.
- Customers: where we act as processor, we make data available to the relevant Customer as controller.
- Third-party platforms: where you or your Customer choose to publish or send video or other data to a third-party platform (such as YouTube, social media, or a league or recruitment platform), including through our integrations. Once received, that data is handled under the platform's own terms and privacy policy, not this Notice.
- Legal requirements: where required by law, court order, or regulatory authority.
- Business transfers: in connection with a merger, acquisition, or sale of assets, subject to appropriate confidentiality and data protection obligations.
- With your consent: where you have specifically agreed to a disclosure.
- Group companies: PlayerData Limited and PlayerData Inc. share personal data within the PlayerData group for operational purposes, including infrastructure, technical support, and engineering. Each entity handles personal data in accordance with this Notice.

We do not sell personal data to third parties. See Section 7 for details of the safeguards in place for international transfers.

7. International Transfers

We may transfer personal data internationally, including: (a) between PlayerData Limited (UK) and PlayerData Inc. (US) for support and engineering purposes; and (b) to service providers and sub-processors that support our Services and are located outside your jurisdiction. In addition, US customer data is currently hosted on UK infrastructure operated by PlayerData Limited. This hosting arrangement may change as our business develops; where it does, we will ensure that appropriate safeguards are in place to maintain the same level of protection.

Where we transfer personal data, we ensure that appropriate safeguards are in place to protect the data in accordance with applicable data protection laws. Depending on the nature and destination of the transfer, we use one or more of the following mechanisms:

- the European Commission's Standard Contractual Clauses for transfers of personal data outside the EEA.
- the UK's International Data Transfer Agreement and/or the European Commission's Standard Contractual Clauses and/or the UK Addendum for transfers of personal data outside the UK.

For further information or to request a copy of the transfer safeguards, contact dataprotection@playerdata.com.

8. Security

PlayerData implements appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, or alteration. These measures include encryption of data in transit and at rest, access controls, regular security testing, and staff training.

Please be aware that the transmission of information via the internet is not always completely secure. Although we will do our best to protect your personal data, we cannot guarantee the complete security of your data transmitted to us electronically; any transmission is at your own risk.

Where PlayerData acts as a processor, security obligations are set out in the relevant DPA. Where video content is recorded for the Video Analysis Services, footage is stored locally on the device prior to upload. Physical security of the camera device and locally-stored content during that period is the responsibility of the Customer.

9. Retention

We retain personal data only for as long as necessary for the purpose for which it was collected, or as required by law. Our standard retention periods are set out below.

Category	Retention period
Customer account details (name, contract terms and invoices)	Duration of contract plus 6 years
Billing and financial records	7 years (legal obligation)
Marketing contact data	Until opt-out, or 3 years from last interaction, whichever is earlier
Website and technical logs	12 months
Performance data from Equipment	Duration of account plus 12 months

Video content, including video overlays and annotations	Until the Customer's agreement ends (or earlier if deleted by the Customer or removed under its storage allowance), except copies held in training datasets
Data Sharing Feature entries (Leaderboard, Recruitment Platform)	Retained while you remain enrolled; removed when you withdraw, when your Customer instructs removal, or when your account becomes inactive.

After the applicable retention period, personal data is securely deleted or anonymised.

10. Cookies

PlayerData uses cookies and similar technologies on its website. Cookies are small files placed on your device that help the website function and allow PlayerData to understand how it is used.

PlayerData uses three categories of cookies:

- **Strictly necessary:** essential for the website and app to operate (e.g. login and session management). These are placed without consent as they are required for the service to function.
- **Analytics:** to understand how PlayerData's Services are used (e.g. Google Analytics, Hotjar). These are only placed with your consent.
- **Advertising:** to serve relevant content and measure campaign effectiveness (e.g. Meta). These are only placed with your consent.

When you visit PlayerData's website, a cookie consent banner will allow you to accept or decline non-essential cookies. You can update your preferences at any time via the cookie settings link in the website footer.

11. Third Parties

Our Services may contain links to other websites, products, or services that we do not own or operate. We are not responsible for the privacy practices of these third parties. Please be aware that this Notice does not apply to your activities on these third-party services or any information you disclose to these third parties. We encourage you to read their privacy policies before providing any information to them.

12. Children

When PlayerData acts as a data processor

PlayerData's Services are deployed primarily by sports clubs, teams and educational institutions to their members, including children. In this context, the Customer is the data controller and is responsible for providing appropriate notices and obtaining any consents required by applicable law before enrolling children in the Services, including, for any Authorised User under 18, any parental or guardian consent required for the recording and use of their image and video (for example through the Video Analysis Services). PlayerData processes children's personal data only on the Customer's documented instructions under the DPA, except as described below.

When PlayerData acts as a data controller

Account activation

Where PlayerData acts as data controller, including where Equipment is purchased directly and when operating Data Sharing Features, the following minimum ages apply:

Jurisdiction	Minimum age without parental consent
UK	13
US	13
EEA	16 (or lower national threshold if applicable)

Recruitment Platform enrolment

Where an Authorised User under 18 is to be enrolled in the Recruitment Platform, PlayerData additionally requires verifiable parental consent regardless of the minimum age threshold above, given the nature of that feature.

If we become aware that we have collected personal data from a child below the applicable minimum age without appropriate consent, we will delete it promptly or seek to obtain consent where permitted by law.

Parents and guardians may exercise rights over their child's data — including access, correction and deletion — by contacting dataprotection@playerdata.com. The general rights described in section 13 apply equally to children's data where PlayerData is the controller.

Product improvement

We may anonymise children's performance data, as we do for other users, so that no individual can be identified, and use the anonymised data for product development, benchmarking and research. We do not use the video of teams that include children under 13 to develop or improve our products.

13. Your Rights

If PlayerData is the data controller of your personal data

Depending on your location, you may have the following rights:

- Access: to receive a copy of your personal data
- Rectification: to correct inaccurate data
- Erasure: to request deletion in certain circumstances
- Restriction: to limit how we process your data
- Portability: to receive your data in a machine-readable format
- Object: to processing based on legitimate interests, or to direct marketing
- Withdraw consent: at any time, without affecting prior lawful processing

To exercise any right, contact dataprotection@playerdata.com.

If you are an Authorised User of a Customer account

Your rights in respect of your data should be exercised with the organisation that is our Customer (usually your club, team or organisation) in the first instance, as they are the data controller. PlayerData will cooperate with the Customer to fulfil data subject requests as required under the DPA.

If you wish your data to be transferred to another club or organisation, please contact your current club or organisation. Because they are the data controller, the decision whether to transfer, what to transfer and to whom rests with them. PlayerData cannot action such a transfer without the Customer's instruction.

PlayerData may also provide an in-app export function through which you can take a copy of your data. The availability of this function depends on your Customer's settings, and does not affect any of the rights described above.

Complaints

If you have a concern about how PlayerData handles your personal data, PlayerData would welcome the opportunity to address it first — please contact dataprotection@playerdata.com.

You also have the right to complain to the relevant supervisory authority for your location. For UK users this is the Information Commissioner's Office at ico.org.uk. For EEA users, this is the data protection authority in your country of residence. For US users, this is the relevant state Attorney General or consumer protection authority; California residents may contact the California Privacy Protection Agency at cppa.ca.gov.

14. US Privacy Rights

PlayerData Inc. serves customers in the United States. US privacy law varies by state and PlayerData monitors its obligations as its US business develops.

PlayerData applies the same data protection standards globally, including the principles of purpose limitation, data minimisation, security, and individual rights of access and correction, regardless of where a user is located.

PlayerData is not a covered entity or business associate under HIPAA. Heart rate data collected through the Equipment does not constitute protected health information within the meaning of HIPAA.

15. Individual Athletes Using PlayerData Directly

Where you have purchased Equipment directly from PlayerData (not through a club or team), PlayerData acts as data controller of your personal data, and all sections of this Notice apply to you directly.

As a direct customer you may, through the PlayerData app:

- Access and view your performance data
- Edit your account and profile information
- Upload additional personal performance data
- Download your data
- Share selected performance statistics on social media

To exercise your data rights or to request deletion of your account, contact dataprotection@playerdata.com.

16. Changes to This Notice

We will post updates to this Notice on our website. For material changes, we will notify Authorised Users directly.

17. Contact Us

PlayerData Limited, 3–5 Melville Street, Edinburgh EH3 7PE

PlayerData Inc., 2 Oliver Street, Boston MA 02109. US callers may also reach us at +1 888-413-6220.

Email: dataprotection@playerdata.com

Version 3.1.2 | Effective Date: 9th November 2026