APEX SPORTS TECHNOLOGY LTD
20 Wenlock Road
London
N1 7GU
United Kingdom
hello@squadzy.app

Squadzy: Data Processing Agreement

Version 1.0 · 13 November 2026

This Data Processing Agreement is incorporated by reference from the order form, so schools do not sign it separately. It applies to pilots that use real personal data as well as to paid contracts.

1. Parties, status and definitions

1.1 This Data Processing Agreement (**DPA**) is between the school or school group named in the order form (**Customer**) and Apex Sports Technology Ltd, company number 17256832, registered office 20 Wenlock Road, London N1 7GU, United Kingdom (**Processor**, trading as Squadzy).

1.2 This DPA applies in the version incorporated by the order form and forms part of the agreement under which Processor supplies the Squadzy service (**Principal Agreement**). The Customer accepts it by signing the order form. No separate signature is needed. It applies to pilots that use real personal data as well as to paid contracts.

1.3 If there is a conflict about the processing of Personal Data, this DPA prevails over the other documents that make up the Principal Agreement. The order of the documents on other matters is set out in the order form. Reference material such as the IT and Security pack is for information only and is not part of the Principal Agreement.

Definitions

Applicable Data Protection Law means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, the EU GDPR where Personal Data of individuals in the EEA is processed, and any other data protection law that applies to a Party in connection with this DPA, in each case as amended.

Controller, **Processor**, **Personal Data**, **Data Subject**, **Processing**, **Personal Data Breach** and **Supervisory Authority** have the meanings given in Applicable Data Protection Law.

Customer Personal Data means the Personal Data described in Schedule 1 that Processor processes on behalf of Customer.

Service means the Squadzy hosted application (web dashboard and mobile application) and related support, as described in the Principal Agreement.

Sub-processor means a third party engaged by Processor to process Customer Personal Data.

Security Measures means the technical and organisational measures in Schedule 4.

Transfer Tool means a valid mechanism for restricted transfers under the UK GDPR or EU GDPR, including an adequacy decision or the standard contractual clauses with the UK

Addendum.

2. Roles

2.1 Customer is Controller and Processor is Processor. Where Customer is a group contracting for several schools, Customer warrants it may instruct Processor for each school whose data is loaded. Each school is a separate tenant.

2.2 Processor will not decide the purposes of Processing Customer Personal Data except as set out in this DPA and the Principal Agreement.

2.3 Customer is responsible for its lawful basis and transparency (including privacy notices to staff, parents and pupils), the accuracy of data it or its MIS provides, and retention decisions beyond Processor's deletion mechanics.

2.4 Processor's privacy contact is Chris Lorimer, data protection lead, chris@squadzy.app. Processor's security contact is Peter Friel, CTO, peter@squadzy.app. Customer's privacy contact is named in the order form.

2.5 For a limited set of its own purposes (platform security, billing, legal compliance and service monitoring) Processor acts as an independent Controller, as the Privacy Policy explains. This DPA does not cover that processing.

3. Instructions

3.1 Processor shall process Customer Personal Data only to provide, secure and support the Service, as documented in this DPA and its Schedules, and on other documented instructions from Customer that are consistent with Applicable Data Protection Law and the Principal Agreement.

3.2 Processor shall tell Customer if it believes an instruction infringes Applicable Data Protection Law, and may suspend that instruction until Customer confirms or amends it.

3.3 The Service is for school sport and activity operations: teams, sessions, attendance, RSVPs, in-product communications, uploaded media and the identity data needed to run those features. Photographs and names of children are Personal Data and are in scope. They are not special-category data only because the Data Subject is a child.

3.4 **Medical information and emergency contacts.** Customer controls which fields its MIS shares with Squadzy through Wonde. Medical conditions are imported only where Customer authorises them in Wonde and switches on the medical import setting in Squadzy, and Customer then instructs Processor to process that information to provide the Service. Medical conditions are special-category data. Medical information from the MIS can include free-text narrative entered by the school. Medication records are not imported by default. Medical conditions imported from the MIS are read-only in Squadzy: the server ignores edits to them, and corrections are made in the MIS and arrive on the next sync. Medical information that a school enters directly in Squadzy remains editable by authorised users. Access is limited on the server by role and team. Coaches can see this information for students in the teams they are assigned to, and directors and other administrators whom Customer authorises have wider access. There is no separate medical-only permission. Customer is responsible for having a condition under UK GDPR Article 9 (or equivalent) and for deciding who it appoints as a coach or director. Processor does not include medical information or emergency-contact details in

requests to its AI provider.

3.4A Emergency contacts and parent details. Squadzy does not import emergency-contact records from the MIS. An emergency contact on a pupil is entered by the school and is optional. Where Customer authorises it in Wonde, Squadzy imports parent and guardian identity and contact details (name, email, phone where available, and parental-responsibility links). Emergency contacts are Personal Data but are not special-category data merely because they are emergency contacts. Processor does not process any other special-category data, such as safeguarding case files or special educational needs records, unless Customer gives a written instruction and a documented feature is enabled.

3.5 **MIS sync.** Identity and contact fields sourced from Wonde are read into the Service and are read-only in Squadzy by default. Corrections are made in the school's MIS and arrive on the next sync. To erase a Wonde-managed person, Customer must stop sharing that person through Wonde and instruct Processor to delete or anonymise the Squadzy record.

3.6 **Write-back.** Customer decides in Wonde what Squadzy can read from its MIS and, where Squadzy supports it, what Squadzy can write back (for example attendance records). Squadzy reads and writes only what Customer has authorised in Wonde. Customer can change or withdraw those permissions in Wonde at any time.

3.7 **Analytics and optional modules.** Processor uses product analytics (Pendo) on the staff dashboard and error monitoring (Sentry) to run and improve the Service. They are not used for marketing. Processor does not use session replay or heatmap tools. Processor does not enable marketing tags on Customer's tenants without Customer's written instruction. AI features and in-app payments are optional and are off unless Schedule 3 shows them as On or Customer switches them on in the Service, in which case the switch is Customer's instruction and Processor records the time, the user who made it and the version of the terms accepted.

4. Security and personnel

4.1 Persons authorised to process Customer Personal Data are bound by confidentiality and have access only as their role needs. Privileged platform access (AWS, deployment, content management) is limited to named accounts, protected by multi-factor authentication where the system supports it, and reviewed periodically.

4.2 Processor shall maintain the Security Measures in Schedule 4 and other measures appropriate to the risk under UK GDPR Article 32, taking into account that many Data Subjects are children.

4.3 Processor is certified under UK Cyber Essentials (certified on 8 October 2026, with renewal due on 8 October 2027). The certificate is available to Customer on request. It is a baseline assurance and is not a statement that each measure in Schedule 4 is separately certified.

4.4 Customer is responsible for school-side access (who is invited, which role they hold, coach-to-team assignments), school-managed devices and networks, and its MIS and Wonde configuration. Multi-factor authentication is available for sign-in but is not mandatory for every school user.

5. Sub-processors

5.1 Customer authorises the Sub-processors in Schedule 2, including those used only if the

related optional module is on. The current list is also published at squadzy.app/legal/subprocessors.

5.2 Processor shall bind each Sub-processor to data protection obligations in substance equivalent to this DPA and remains liable to Customer for each Sub-processor's processing, subject to clause 11.

5.3 Processor shall give Customer at least 30 days' notice of a new Sub-processor, by email to Customer's privacy contact or an in-product notice. A shorter notice is allowed only where a change is needed sooner for security or continuity, and then Processor shall notify as soon as practicable.

5.4 Customer may object on reasonable data protection grounds within 14 days of notice, and the Parties shall discuss in good faith. If Processor cannot reasonably continue the Service or the affected feature without that Sub-processor, either Party may end the affected feature or the Principal Agreement on written notice without liability for that ending alone, and clause 9 applies.

5.5 A Sub-processor's own further processors are permitted where covered by that Sub-processor's DPA and a Transfer Tool.

6. International transfers

6.1 The production database, media files and database backups are stored in AWS in Singapore (ap-southeast-1), as stated in Schedule 1. Staging and test environments are in AWS Tokyo (ap-northeast-1) and hold dummy data only. Real school data is never copied into staging or test environments. Web traffic passes through CloudFront and WAF edge services that inspect requests globally, and the Sub-processors in Schedule 2 process data in the places their own terms describe.

6.2 Some Sub-processors (such as identity, error monitoring, analytics and push notifications) may process Personal Data in the United States or other countries. Processor shall not transfer Customer Personal Data outside the UK or, where it applies, the EEA unless the destination has an adequacy decision, a Transfer Tool is in place, or another valid condition under Applicable Data Protection Law applies.

6.3 Customer instructs Processor to make the transfers needed to provide the Service, including through Sub-processor DPAs that incorporate a Transfer Tool. Where UK GDPR or EU GDPR applies to Customer Personal Data and it is transferred to a country without an adequacy decision, the Parties shall put in place, before the transfer, the UK International Data Transfer Addendum to the EU standard contractual clauses or the UK International Data Transfer Agreement, as applicable.

7. Data Subject rights and assistance

7.1 Processor shall assist Customer, by appropriate technical and organisational measures and as far as possible, to respond to requests to exercise Data Subject rights.

7.2 If a Data Subject contacts Processor about Customer Personal Data, Processor shall redirect them to Customer and notify Customer without undue delay, unless the law prevents it.

7.3 Access, correction, deletion, portability, restriction and objection are carried out on Customer's instruction and only within that school's tenant. Processor's engineers carry out the

extract or deletion.

7.4 Processor shall assist Customer with its obligations under UK GDPR Articles 32 to 36 (security, breach notification, impact assessments and prior consultation), taking account of the information available to Processor.

7.5 Target times: acknowledgement within 5 working days, and completion within 30 days of a complete instruction, or longer where the law allows Customer an extension.

8. Personal Data Breach

8.1 Processor shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data, and in time for Customer to meet any 72-hour duty to notify a Supervisory Authority. Processor shall notify Customer's privacy contact within 24 hours of confirming a Personal Data Breach affecting that Customer. A breach is confirmed when Processor has established that a Personal Data Breach affecting Customer Personal Data has occurred. Processor shall investigate any suspected Personal Data Breach promptly and shall not delay confirming a breach to wait for complete information. In any event, Processor shall notify Customer's privacy contact no later than 48 hours after Processor first detects indications that reasonably suggest a Personal Data Breach affecting that Customer, even if its investigation is not complete.

8.2 The notice shall include, as far as then known: what happened, the categories and approximate number of Data Subjects and records, the likely consequences, the measures taken or proposed, and a contact point. Processor shall provide updates as it learns more.

8.3 Processor shall not notify a Supervisory Authority or Data Subjects for Customer unless Customer instructs it in writing or the law requires it.

9. Return and deletion

9.1 During the term Customer can export or delete data in the Service where that function exists, or by written instruction.

9.2 When the Service ends for a tenant, Customer has 30 days after the end date to export its data (the **export period**), or to ask Processor for a copy in a reasonable machine-readable format. Processor shall then delete the production Customer Personal Data within a further 30 days, or earlier if Customer instructs it in writing, unless the law requires storage.

9.3 Where Customer asks for an individual to be deleted during the term (for example a pupil), the export period does not apply, and Processor shall delete that individual's production data within 30 days of a valid instruction.

9.4 The following are not deleted at the same moment as production data: (a) database backups, which are kept for 14 days and so expire within 14 days after the production deletion, meaning backup copies of a departed tenant's data may remain for up to about 74 days after the end date; (b) application and security logs, kept for up to 12 months, which may contain user identifiers (IDs, not names or emails) and are not used to provide the Service to the school after deletion, and load balancer access logs, kept for 90 days; and (c) copies held by Sub-processors under their own DPAs. For Clerk, Processor removes the school's organisation access at offboarding and disables or deletes accounts on Customer's instruction. For Sentry, data is kept for the vendor's operational retention period and is not a system of record.

9.5 Processor shall confirm deletion in writing on request.

10. Information and audit

10.1 Processor shall give Customer the information reasonably needed to show compliance with this DPA, and shall keep records of processing and cooperate with a Supervisory Authority on request.

10.2 Customer's audit rights are: (a) written questionnaires; (b) the Cyber Essentials certificate and other security assurance documents Processor holds; and (c) one remote audit in any rolling 12 months on at least 20 working days' notice, in business hours, without unreasonably disrupting the Service, and subject to confidentiality.

10.3 On-site audits of AWS or other Sub-processor data centres are not offered. Customer may rely on the Sub-processor's published reports.

10.4 If an audit finds no material breach, Customer bears its own costs and Processor's reasonable costs. If it finds a material breach, Processor bears its own audit costs to the extent the breach caused them.

10.5 Processor need not disclose information that would compromise the security of the Service or other customers, or that is legally privileged.

11. Liability

11.1 Nothing in this DPA limits liability that cannot be limited by law, including death or personal injury caused by negligence, or fraud.

11.2 Subject to clause 11.1, each Party's total liability under or in connection with this DPA in any contract year is limited to the greater of (a) the annual fees payable by Customer under the order form for that contract year and (b) £25,000. A contract year is each 12 months starting on the start date or a renewal. This limit and the limit in the Master Terms are one combined limit for the Principal Agreement as a whole. They are not added together.

11.3 Subject to clause 11.1, Processor is not liable for Customer's instructions or unlawful Customer data, school-side access misconfiguration, MIS or Wonde content, or loss of profit, goodwill or indirect or consequential loss.

11.4 Administrative fines on Customer as Controller are Customer's responsibility except to the extent Processor's breach of this DPA caused them, and then only within clauses 11.1 to 11.3.

12. Term, changes and law

12.1 This DPA starts on the order form date and continues until Processor has deleted or returned Customer Personal Data under clause 9. Clauses 4, 9, 11 and 12 survive.

12.2 Processor may publish a new version of this DPA. A new version applies to Customer only (a) from the next renewal or extension, or (b) 30 days after Processor emails notice of a material change to Customer's privacy contact, unless Customer objects in that time, in which case the version Customer signed continues to apply for the rest of its term. Changes to the sub-processor list follow clause 5 instead.

12.3 This DPA is governed by the laws of England and Wales, and the courts of England and

Wales have exclusive jurisdiction, unless the order form says otherwise.

12.4 If a provision is invalid the rest remains in effect.

Schedule 1: Details of processing

Item	Detail
Subject matter	Hosting and operation of Squadzy for school sport and activities
Duration	Term of the Principal Agreement plus the export and deletion periods in clause 9
Nature	Collection, storage, retrieval, display, transmission, backup, logging and deletion. Optional MIS sync through Wonde (including write-back, where supported and authorised by the school in Wonde), payment metadata and AI processing when those modules are on
Purpose	Providing the Service to the Customer's school tenant(s)
Data Subjects	School staff (directors, coaches, administrators), pupils and students, parents and guardians, other contacts the Customer enters
Personal Data	Identity and contact details (name, email, user ID, organisation membership); school and team membership; session, attendance and RSVP data; in-product messages; uploaded media, which may include images of children; device and push tokens; technical logs (user ID, tenant ID, path, time, and source IP in edge and access logs); staff usage analytics on the staff dashboard. Card numbers are never stored by Processor
Special-category data	Medical conditions only where the Customer authorises them in Wonde and switches on the medical import setting, or enters them directly (clause 3.4). Emergency contacts, which the school enters, are Personal Data but not special-category data. Nothing else unless Customer gives a written instruction
Frequency	Continuous while the tenant is active
Storage location	Production database, media and backups: AWS Singapore (ap-southeast-1). Staging, with dummy data only: AWS Tokyo (ap-northeast-1). Edge protection through CloudFront and WAF inspects requests globally. Other locations: see Schedule 2

Schedule 2: Sub-processors

Locations are summaries. The vendor's DPA and Transfer Tool govern.

Supplier	Role	Customer Personal Data	Used
Amazon Web Services	Cloud hosting in Singapore (application, database, file storage, logging and secrets). CloudFront and WAF edge services inspect traffic globally	Application data, media, logs	Always
Clerk, Inc.	Sign-in, organisations, MFA, session history, and sign-in and invitation emails	Name, email, user ID, organisation membership, session metadata	Always
Functional Software, Inc. (Sentry)	Error and crash monitoring (ingested in the EU), with PII scrubbing on and session replay off	Technical events	Always
Pendo.io, Inc.	Product analytics and in-app guides on the staff dashboard (EU region where configured)	Staff identifiers, pages viewed and actions taken	Always
Expo (Expo Application Services)	Mobile builds and push delivery	Device and push tokens	Always
Upstash, Inc.	Technical shared state (rate limits, locks, debounce) and a short-lived authentication cache	Rate-limit, lock and debounce keys (IDs and counters), and a short-lived authentication cache containing user ID, email, username, role, role type, document ID and school ID and name	Always
Wonde Ltd	School MIS sync, as authorised by the school in Wonde	Pupil, parent and guardian identity and contact details, MIS identifiers, and where Customer authorises them medical conditions	If Wonde sync is On
Stripe, Inc.	Card payments, using Stripe Connect on the school's own account	Payer name and contact, child's name, item, amount, internal reference. Card details go to Stripe only	If payments are On
Anthropic, PBC	AI drafting assistant	Request-scoped text in which names are replaced	If AI is On

Supplier	Role	Customer Personal Data	Used
		by aliases (for example Child_1). Medical, emergency-contact, email, phone and address data are removed before requests are sent	

Microsoft and Google, when used only as the school's own single sign-on provider, act for the Customer and are not Processor's Sub-processors.

Schedule 3: Optional modules

The order form shows each module as On or Off. All optional modules are Off unless the order form says On or the Customer switches them on in the Service.

Module	Default	Effect when On
Wonde MIS sync	Off	Wonde becomes a Sub-processor. Identity fields come from the MIS and are read-only (clause 3.5). Parent and guardian contact details arrive if the Customer authorises them. Medical conditions arrive only if the Customer authorises them in Wonde and switches on the medical import setting. Emergency-contact records are not imported
MIS write-back	Customer's choice in Wonde	Squadzy writes back only what Customer has authorised in Wonde (clause 3.6)
Stripe payments	Off	Stripe becomes a Sub-processor. Processor never holds funds or stores card numbers. The school is the merchant
AI features	Off	Request-scoped snippets may leave the AWS tenant boundary to the AI provider, with names replaced by aliases and medical, emergency-contact and contact details removed first. Output is draft-only and reviewed by staff

Schedule 4: Technical and organisational measures

Processor maintains at least the following.

1. **Tenant isolation.** Each school is a tenant. API requests are scoped by school. Cross-tenant access is denied in application policy and by PostgreSQL row-level security.
2. **Access control.** Role-based access within a tenant (director, coach with assigned teams, parent linked to children, student). Medical information is limited by role and team assignment (clause 3.4). Privileged cloud and CMS access uses named accounts and multi-factor authentication, with periodic review.
3. **Encryption.** TLS in transit. Encryption at rest for the database and object storage. Secrets held in AWS Secrets Manager, not in source control.

4. **Network.** The production database is not on the public internet. Public entry points are protected by CloudFront and WAF.
5. **Logging.** Application and security logs use user ID and tenant ID, not school names or emails, and are kept for 12 months. Structured events are logged when a request is denied by tenant policy, with tenant ID, user ID, path and method. Third-party identity-provider records may be kept for different periods. Load balancer access logs are kept for 90 days. Clerk holds sign-in history.
6. **Development.** Changes are made through version control and tested automatically, including tenancy and security tests, before release. Dependencies are kept up to date under a documented patch policy that sets timescales by severity.
7. **Backups.** Automated database backups are kept for 14 days. A restore test will be completed and evidenced before go-live, and repeated at least annually after that.
8. **Incidents.** A documented incident process including GDPR assessment and Customer notification under clause 8.
9. **Vendors.** Sub-processors only as listed in Schedule 2, with a vendor DPA in place before they process Customer Personal Data.
10. **Staff devices.** Laptops that may access production use full-disk encryption and baseline OS security. Customer Personal Data is not stored as the system of record on staff laptops.
11. **Assurance.** UK Cyber Essentials certification. This is baseline assurance and does not separately certify each measure above.

These measures may change if the overall level of protection is not reduced.