STS

Data processing

Between an academy and Sleek&Tech System Ltd

Every market — **draft for review**

Sleek&Tech System Ltd

RC 9771734 · Nigeria

sleektechsport.com · info@sleektechsport.com

Not legal advice, and not to be signed as it stands. Drafted 9 August 2026 and extended 12 August with a schedule for every market this product can already be sold into. The sub-processor list is the real one and the security measures are the controls that exist. **A DPA cannot make a business lawful in a country** — Annex E lists what no contract supplies, and marks which gates have a live customer behind them today.

Data Processing Agreement

Between the Academy (the Controller) and Sleek&Tech System Ltd (the Processor)

Version 1.0 · 9 August 2026 · Extended to every market 12 August 2026 · POPIA transfer clause added 15 August 2026 · jsDelivr removed from Annex A 30 August 2026

> **This agreement takes effect when an Academy accepts our terms**, and the data processing terms in those terms state that this is the required processing agreement where the GDPR, UK GDPR, POPIA, the NDPR or a comparable law applies.
>
> **Every factual claim about the system here has been checked against what the system actually does.** The sub-processor list is the real one, the retention periods match `terms.html`, and the security measures are the controls that exist rather than the ones we would like to have. Where something is not in place, it is named in Annex E rather than left for a reader to discover.
>
> **A DPA cannot make a business lawful in a country.** It is the contract between us and an academy, and it is necessary almost everywhere. It is not sufficient anywhere. Several countries additionally require a registration, a licence, or a locally-appointed representative *before* the first customer is served — none of which a contract supplies. Those are collected in **Annex E**, deliberately separated from the clauses, because the honest answer to "does this document make us qualified to operate there" is no, and Annex E is what would.

Why this document exists at all

An academy that uses Sleek&Tech-Sport is handing us the names and dates of birth of children, and their parents' phone numbers. In law that academy remains responsible for those records. We hold them on the academy's behalf, and that relationship is supposed to be written down before it starts, not after something goes wrong.

It is also a practical document. Half of it is a description of who can see what and what happens when something breaks, which is worth having in writing whether or not a regulator ever asks.

---

0. How this document is built, and which parts apply to you

The clauses in **§1–§13** apply to every Academy, in every country. They are written to satisfy the common core that data protection statutes almost universally require of a processor contract:

purpose limitation, confidentiality, security, sub-processor control, assistance with data subject rights, breach notification, deletion, and audit.

Annex C then adds a country schedule. Where a schedule conflicts with the main body, the schedule wins for that Academy. Attach the schedule for:

- the country in which the Academy is established; **and**
- any country where the Academy's students and their families are, if different.

Those are usually the same country and occasionally are not — a coach in Lagos running a camp for families in London engages both.

> **This was a gap, and it has been closed — with a caveat worth reading.**
>
> Until 12 August 2026 the platform did not record which country an Academy was in. It recorded a *locale*, which is not the same thing and is not a proxy for it. The registration form now asks, in every language the site reads in, and the answer is stored as an ISO 3166 country code on the Academy record.
>
> **The first draft of the table below was built from locale and it was wrong.** It said Nigeria 11, United States 6. One account carries the `en-US` locale, the `USD` currency and the city "Lagos" — a Nigerian academy that the locale reading called American, which is precisely the error that would have attached the wrong schedule, the wrong regulator and the wrong breach deadline to a real customer. The corrected table is below.

Where Academies actually are today

12 August 2026. All nineteen Academies are placed, and none of them by a guess. The founder went through the list by name — he has spoken to every one of these coaches directly — and every row is now sourced from him rather than from a script reading a free-text city.

COUNTRY	ACADEMIES	SOURCE	SCHEDULE
Nigeria	12	founder	C1
United States (Texas)	5	founder	C5
South Africa	2	founder	C4
Total	**19**		

Each row records *who said so*, and it is worth explaining why a bare country was not enough. Three qualities of answer exist — `academy` (chosen by the Academy itself, the only authoritative one), `operator` (the founder, from personal knowledge) and `inferred` (guessed from the city, checked by nobody).

That distinction earned itself immediately. Asked to place the remainder, the founder said "the rest are in Nigeria" — a sentence which, applied as written, would have moved two Texan Academies to Nigeria, and with them the regulator their families complain to, the deadline we owe after a breach, and the age at which a person stops being a child. Both were queried back by name and corrected. A third, whose city field reads "19000" on a South African locale, was held back for the same reason and confirmed separately.

None of that would have been visible if the record stored only the answer.

An Academy's own statement outranks the founder's, and that is what the registration form now collects. Every Academy from 12 August onward states its own country.

24 August 2026. Read from the production database, not remembered: Nigeria 17, United States 6, South Africa 2, Qatar 1 — twenty-six Academies. Qatar is new that day (Abass tennis Academy, Doha, signed up 24 August), and takes schedule C8 below. Every Academy now sits inside a written schedule except the EEA and the UK, where no Academy has ever been; those two schedules remain written in advance so that the answer to a prospective customer is a document rather than a delay — and so the gates in Annex E are visible *before* somebody signs up, not after.

---

1. Parties

Controller: the academy, club, school or individual coach named on the account (the "Academy"). In some countries this role has a different name — *responsible party* under POPIA, *data fiduciary* under India's DPDP Act, *business* under Californian law. The country schedule says which, and the role is the same one.

Processor: Sleek&Tech System Ltd, a company registered in Nigeria with the Corporate Affairs Commission under number **RC 9771734**, incorporated 13 August 2026 ("we", "us"). Called *operator* under POPIA, *data processor* under the DPDP Act, *service provider* under Californian law, *entrusted party* under China's PIPL.

This agreement is incorporated into the Terms of Service. Where the two disagree on the handling of personal data, this document governs.

---

2. What we do with the data, and for how long

Subject matter. Providing the Sleek&Tech-Sport platform: a roster, attendance register, invoicing, booking and check-in pages, and reports.

Duration. For as long as the Academy has an account, plus the retention period in §10.

Nature and purpose. Storing, organising, retrieving, transmitting and deleting records the Academy enters or which its students and their parents submit through the Academy's own booking and check-in links. We process this data **only to provide the service to that Academy**.

We do not:

- sell personal data, or share it with anyone for their own purposes;
- retain, use or disclose it for any purpose other than performing this service, including outside our direct business relationship with the Academy;
- use one Academy's data to serve another;
- combine it with data received from anyone else, except as needed to run the service for that Academy;
- use the data to train machine-learning models;
- use children's data for marketing, profiling, targeted advertising, or any form of behavioural tracking.

(The second, fourth and last of those are worded to meet the specific prohibitions Californian and other US state statutes require a service provider contract to contain, and India's DPDP Act §9(3). They are also simply true.)

---

3. Categories of data and of data subject

Data subjects: students of the Academy — **many of whom are children** — their parents or guardians, and the Academy's coaches and staff.

Categories of personal data:

Students	Name, **age**, level or grade, attendance history, session notes written by a coach, lesson balances, invoices
Parents / guardians	Name, phone number, email address, messages sent through the check-in page
Coaches and staff	Name, email address, phone number, role, and where the Academy uses payroll features, payslip records

Special category data. The platform is not designed to hold health data, and nothing asks for it. A free-text notes field could receive it if a coach types it there. Academies should not record medical information in notes; if that changes, this agreement needs revisiting, because health data carries obligations this document does not currently address.

Children. This is the sensitive part and it is why §7, §8 and every country schedule are written the way they are. The Academy is responsible for having a lawful basis for entering a child's

details — usually the parent's consent or the Academy's contract with the family — and for telling families that a third-party system is used. We provide the plain-English description at `/privacy.html` for that purpose.

Two design decisions reduce what the Academy has to defend, and both are facts about the running system rather than promises:

- **The player check-in page does not ask a child for an email address or an age.** It asks for a name, an enjoyment slider and a free-text message. The parent version asks for contact details, because that is an adult supplying their own. This matters most under COPPA and India's DPDP Act, which treat collection *directly from* a child as a distinct act.
- **We do not collect a child's date of birth.** From 20 August 2026 the panel asks for an **age**, after Academies were asked and said they wanted the number or nothing. A date of birth is an identity token used to verify people and to recover accounts; an age answers the only question the platform asked it — is this person a child, so must a parent have agreed — and is far less use to anyone who should not have it. Dates collected before that date were converted to ages in place and then **deleted on the same day**. None remain.
- **The age is not visible to every coach.** It is held in a separate table readable only by the Academy's owner and admin.

The age at which a person stops being a child for these purposes is **not uniform** — 13 in the United States for COPPA, 13 to 16 across the EEA, 18 under India's DPDP Act and for much of Nigeria's guidance. The country schedule states it. Nothing in the platform assumes a single number.

---

4. The Academy's instructions

We process personal data only on the Academy's documented instructions. Using the platform's features **is** the instruction: adding a student instructs us to store that student; sending an invoice instructs us to transmit it.

We will tell the Academy if an instruction appears to breach applicable data protection law, and may decline to act on it.

Where we are required by a law that applies to us to process the data otherwise, we will tell the Academy before doing so unless that law forbids telling them.

---

5. Confidentiality

Access is limited to people who need it to run or support the service, each of whom is bound by confidentiality. In practice this is a very small number of people, and support access to an Academy's records happens only when the Academy asks for help with a specific problem.

6. Security

The measures are listed in **Annex B**, and `SECURITY.md` in the source repository describes them in more detail, including what is *not* yet done. Two points belong here rather than in an annex:

Separation between academies is enforced by the database, not by the application. Every table carrying Academy data has row-level security, and the tables holding children's records additionally have `FORCE ROW LEVEL SECURITY`. A bug in the panel cannot show one Academy another's roster, because the panel is not what decides.

We do not hold card details. Where an Academy takes payment from a family, that happens through the Academy's own bank details or payment link, printed on the invoice. The money does not pass through us.

---

7. Sub-processors

The Academy authorises the sub-processors in **Annex A**. Each is engaged under written terms imposing data protection obligations no less protective than these, and we remain liable to the Academy for their performance.

Changes. We will give at least **30 days' notice** before adding or replacing a sub-processor. If the Academy objects on reasonable data protection grounds, it may terminate without penalty and take a full export of its data.

---

8. International transfers

Data is stored in **Canada** (Supabase, on AWS `ca-central-1`) and served through infrastructure that may process it in other countries. Email leaves through a provider in the United States.

For almost every Academy on this platform, this is a cross-border transfer, and **the correct mechanism differs by country**. It is set out in the country schedule rather than here, because a single sentence covering all of them would be wrong for most of them.

Two facts that make several of those schedules easier, and one that does not:

- Canada holds an **EU adequacy decision** and a **UK adequacy** finding, for organisations subject to PIPEDA. That is favourable but must not be assumed to close the point: adequacy attaches to the *recipient organisation*, and whether a US-incorporated provider storing data in a Canadian AWS region is itself subject to PIPEDA is a question we do not treat as settled, and we do not rely on it as the basis for any transfer.
- The **onward transfer to the United States** for email is the harder leg, not the Canadian one.

We will not move the primary data store to another country without notice under §7.

9. Assisting the Academy

Data subject rights. Where a parent asks the Academy for a copy of their child's records, for a correction, or for deletion, the Academy can do all three itself from within the panel — export at any time, edit any record, delete a student. Where it cannot, we will assist within **10 working days** of a written request.

Breach notification. If we become aware of a personal data breach affecting an Academy's data we will notify that Academy **without undue delay and in any event within 48 hours**, with what we know: what happened, which categories of data and roughly how many people are affected, what we are doing, and what the Academy may need to do. Regulator and parent notification are the Academy's decisions to make as controller; we will give them what they need to make them.

The Academy's own deadline to its regulator is shorter in some countries than others, and the country schedule states it. Ours is set at 48 hours so that the Academy has time left to meet a 72-hour obligation. Whether the business can actually meet 48 hours is kept under review as the platform grows.

Impact assessments. We will provide reasonable information to help the Academy complete a DPIA, which is likely to be required given children's data.

---

10. Deletion and return

The Academy can **export everything, at any time, from the panel, without asking us** and without the export being degraded or delayed.

On termination we keep the data available for export for **30 days**, then delete it from live systems. Backups are deleted on their own rolling cycle and are not restored except to recover the service. If the Academy asks in writing for earlier deletion, we will do it.

---

11. Audit

We will make available the information reasonably needed to demonstrate compliance with this agreement. Given the size of the business, this normally means answering written questions and sharing `SECURITY.md`, rather than an on-site audit. The Academy may audit no more than once a year unless a breach or a regulator requires otherwise, at its own cost, on 30 days' notice.

---

12. Liability

12.1 What is never limited. Nothing in this agreement limits or excludes either party's liability for death or personal injury caused by negligence, for fraud or fraudulent misrepresentation, or for

anything else that the law applying to that Academy does not permit to be limited. Where a country schedule in Annex C makes something unlimitable, that schedule governs.

12.2 Our cap. Subject to 12.1, our total liability to the Academy arising out of or in connection with this agreement, in any twelve-month period, is limited to the **greater** of:

- the fees the Academy paid us in the twelve months before the event giving rise to the claim; and
- **US$1,000**, or the equivalent in the Academy's own billing currency.

The floor matters more than the cap while the platform is free. A limitation to the fees paid is a limitation to nothing when the fees are nothing, and a cap of nil is the kind a court is most likely to strike out — which would leave us with no cap at all. A real floor is better protection than an unenforceable one, and it is the honest thing to show an Academy that is trusting us with children's records.

12.3 What we are not liable for. Subject to 12.1, neither party is liable for loss of profit, loss of business, loss of goodwill, or indirect or consequential loss. We are not liable for loss of data to the extent it results from the Academy not taking the exports this platform makes available to it at all times, without charge and without asking us — see §10.

12.4 The Academy's side. The Academy is responsible for having a lawful basis for the personal data it enters, for the accuracy of that data, and for the instructions it gives us. Where a claim against us arises from data the Academy had no basis to hold, the Academy is responsible for it. This is not a cap on them; it is the counterpart of §4, which says we act on their instructions.

12.5 Where the Standard Contractual Clauses apply. Where the EU or UK SCCs are attached under schedule C2 or C3, those clauses carry their own liability and third-party beneficiary provisions and **this section does not cap them**. A data subject's rights under the SCCs are theirs, not the Academy's to limit and not ours to reduce by contract.

> **On the figure and the shape of the cap.**
>
> The **figure** in 12.2 is a commercial decision — US$1,000 is a floor chosen so that the limit is a real number rather than one that computes to nothing while the product is free. It is open to negotiation with an Academy large enough to want a different one.
>
> As drafted, 12.2 caps only us; 12.3 is mutual. We will discuss a mutual cap in 12.2 with any Academy that asks.

13. Governing law

The law and jurisdiction stated in the Terms of Service, save where an Academy's own data protection law mandates otherwise, and save where an attached schedule specifies a different governing law for that schedule — which the EU SCCs do.

Annex A — Sub-processors

SUB-PROCESSOR	WHAT THEY DO	WHERE	DATA THEY SEE
Supabase (on AWS)	The database and authentication. This is where the records live.	Canada, `ca-central-1`	All Academy data
Vercel	Hosts and delivers the panel, booking and check-in pages, and the API functions	Global edge; functions in the region Vercel assigns	Data in transit; request logs
Resend	Sends email — welcomes, invoices, booking alerts	United States	Recipient address and the content of that email
Anthropic	Drafts a suggested message for a coach to edit, **only when a coach presses that button**	United States	A first name and the coach's own prompt. No surname, contact details, age, attendance history or invoice.

jsDelivr was removed from this Annex on 30 August 2026. That content delivery network served the Supabase JavaScript library to the browser, and so received the IP address of anyone who opened the panel or a booking link — never any Academy data. The library is now served from our own origin and the request no longer leaves it, so **a visitor's browser now contacts no third party at all**. Clause 7 requires 30 days' notice before **adding or replacing** a sub-processor; removing one triggers nothing. It is recorded here anyway, because an Annex that only ever grows is not a record of who sees your data.

Anthropic is currently switched off — the API key is not configured, so no data reaches it at all. It remains listed because enabling it is a configuration change rather than a code change, and an Academy should know before it happens.

Flutterwave became an active sub-processor on 8 September 2026, when the platform began taking subscription payments by card. It receives an Academy's own name, billing email address and the amount of its subscription. **It receives no data processed on an Academy's**

behalf — no learner, no family contact, no attendance, no invoice — and no card detail reaches this platform at any point. It processes in Nigeria.

The 30 days' notice required by §7 was not given before it was enabled, and that notice has not been issued. It is recorded here in those terms rather than as a quiet addition to the table, because a notice period exists so an Academy can object while objecting still changes something. An Academy that would rather not have its subscription handled this way can pay by bank transfer instead, which needs no notice period.

Where the edge is. Vercel's "global edge" is honest but unhelpfully vague for a schedule that turns on geography. For an Academy whose law restricts transfers, the open question is whether edge execution constitutes a transfer to each region it runs in, or whether only the region holding data at rest counts. We do not rely on either reading: the transfer bases in the country schedules are written to cover the wider one.

Annex B — Technical and organisational measures

- Encryption in transit (TLS) for every connection; encryption at rest for the database.
- **Row-level security on every table**, with `FORCE ROW LEVEL SECURITY` on those holding children's records. Tenant separation is enforced by the database, not by application code.
- Access to production data restricted to the smallest possible number of people.
- Service-role credentials held only server-side; the key shipped to browsers is a publishable key with no privileged access.
- Authentication by email and password with hashed credentials; roles within an Academy (owner, admin, coach) limit what each person can see, including hiding a child's age from coaches who do not need it.
- Client-side error reporting that **scrubs email addresses, phone numbers and long digit strings** before an error leaves the browser, and never sends the page's query string.
- **Push notifications carry no message text.** These records name children, and a notification payload sits on a third-party service and appears on a lock screen anyone can read.
- Daily automated backups (Supabase Pro).
- An audit trail of administrative actions, on five tables, which cannot be edited or deleted including by us.
- A documented restore procedure (`docs/RESTORE-DRILL.md`).

Restore, tested. On 9 August 2026 a backup was restored to a separate project and checked: recovery took about 7 minutes, the records came back complete, and — the part that matters for this agreement — every row-level security policy came back with them, so separation between academies survived the restore rather than merely the rows.

Recovery point. Backups are taken daily, so **up to 24 hours of data can be lost**. The drill confirmed this rather than assumed it: two academies that had signed up that morning were absent from the most recent backup entirely. Nothing in this agreement or the Terms of Service should be read as promising a shorter window unless point-in-time recovery is enabled, in which case this paragraph must be updated.

Annex C — Country schedules

Attach the schedule for the Academy's country. Where a schedule says something different from §1–§13, the schedule governs for that Academy.

Each schedule states five things: the statute, the regulator, what the law calls the two parties, what it adds to the main body, and the transfer mechanism for data leaving that country for Canada and the United States.

C1 — Nigeria

17 Academies as of 24 August 2026. Our own country of registration.

Law	Nigeria Data Protection Act 2023, and the NDPC's implementing directive
Regulator	Nigeria Data Protection Commission (NDPC)
Roles	Data controller / data processor
Child	Under 18. Parental consent is required, and the Act is strict about it.
Breach	The Academy notifies the NDPC within 72 hours of becoming aware

What this schedule adds.

1. We process only on the Academy's instructions, keep the data confidential, apply the measures in Annex B, and assist with data subject requests — as in the main body, which was written to the Act's processor requirements.
2. **Registration. Granted.** The Act requires a data controller or processor *of major importance* to register with the NDPC. **Sleek&Tech System Ltd is registered under NDPC/DCP/14079.** Granted in August 2026 in the business name the platform launched under, and transferred to the company on 14 August 2026 with the same registration number. This paragraph read "submitted, approval pending" until the day it was granted. An Academy that is itself of major importance has its own registration obligation, which is the Academy's and not ours.

3. **Transfers.** Data leaves Nigeria for Canada and the United States. The Act permits transfer on several bases; the one we rely on is stated in this schedule and must be settled before this schedule is signed. Do not assume adequacy — the NDPC's list of adequate countries is the thing to check, not an assumption about Canada's reputation.
4. **Data Protection Officer. Appointed and registered with the NDPC.** Contactable at info@sleektechsport.com, and named in the privacy policy so a data subject can reach them without going through us first.

C2 — European Economic Area

No Academies today. This schedule is a gate, not a description.

Law	Regulation (EU) 2016/679 (GDPR)
Regulator	The Academy's national supervisory authority
Roles	Controller / processor
Child	Between 13 and 16 depending on the member state, for consent to information society services
Breach	The Academy notifies its authority within 72 hours

What this schedule adds.

1. **Article 28(3) terms.** §§2, 4, 5, 6, 7, 9, 10 and 11 of the main body are written to contain each of the elements Article 28(3) requires, and are listed here by number so they can be checked against the article rather than taken on trust.
2. **Standard Contractual Clauses.** Commission Implementing Decision (EU) 2021/914, **Module Two** (controller to processor) between the Academy and us, and **Module Three** (processor to processor) for the onward leg to our sub-processors, must be executed and annexed. **They are not in place.**
3. **Transfer impact assessment.** Required alongside the SCCs. Not done.
4. **Article 27 representative.** We are established in Nigeria, not the EEA. If we offer the service to Academies in the EEA we must appoint a representative *in* the EEA in writing. **Not appointed.** This is a cost and a contract, not a clause.
5. **Article 30(2) records.** We must keep a record of processing carried out on behalf of controllers. Annex A and §§2–3 are most of it; it should be maintained as its own document.
6. **A DPIA is likely required of the Academy** given children's data at scale, and we assist under §9.

> **Until items 2, 3 and 4 are done, we should not accept an EEA Academy.** That is a commercial decision written down deliberately, because the alternative — taking the signup and sorting it out afterwards — is how a small company acquires its first regulatory file.

C3 — United Kingdom

No Academies today.

Law	UK GDPR and the Data Protection Act 2018
Regulator	Information Commissioner's Office (ICO)
Roles	Controller / processor
Child	13, for consent to online services
Breach	The Academy notifies the ICO within 72 hours

What this schedule adds. As C2, with three differences:

1. The transfer instrument is the **International Data Transfer Agreement (IDTA)**, or the UK Addendum to the EU SCCs where those are already in place. **Not in place.**
2. A **UK representative** under Article 27 of the UK GDPR, separate from any EEA one. **Not appointed.**
3. The ICO's **Children's Code** (Age Appropriate Design Code) applies to a service children will plainly use. It is a code of practice rather than a statute, and the ICO enforces against it. The design decisions in §3 — no email or age asked of a child, the age restricted, no text in notifications, no behavioural tracking of anyone — were made with it in mind. A gap analysis against its fifteen standards has **not** been done.

C4 — South Africa

2 Academies.

Law	Protection of Personal Information Act 4 of 2013 (POPIA)
Regulator	Information Regulator (South Africa)
Roles	Responsible party / **operator**
Child	Under 18. §35 prohibits processing a child's data except on specific grounds, of which parental consent is the usual one.
Breach	§22 — notify the Regulator and the data subject as soon as reasonably possible after discovery

What this schedule adds.

1. **§20–21 require a written contract** between the responsible party and the operator, obliging the operator to secure the data and to process only with the responsible party's knowledge or authorisation. This agreement is that contract; §§4, 5 and 6 are the operative parts.
2. **§21(2) requires the operator to notify the responsible party immediately** where there are reasonable grounds to believe personal information has been accessed by an unauthorised person. Our §9 window of 48 hours is **not "immediately"**, and for a South African Academy the schedule overrides it: we will notify immediately on becoming aware, and follow with detail as we have it.
3. **§72 transfers.** Personal information may leave South Africa only on one of the listed bases — binding rules, a binding agreement with the recipient providing an adequate level of protection, the data subject's consent, or the transfer being for the data subject's benefit where consent is impracticable. Our basis is the agreement one, and the operative wording is **C4.1 below**.

C4.1 — The §72 transfer clause

This clause exists because §72(1)(a) does not accept a statement that a contractual basis is being relied on. It requires the agreement itself to do two specific things, and a paragraph saying "our basis is contractual" does neither. So this is written as operative terms rather than as description.

The transfer. The Academy is the responsible party and is situated in South Africa. We are the operator. Personal information collected by the Academy is transmitted to us and held at rest in **Canada** (Supabase on AWS `ca-central-1`); is processed in transit by **Vercel**; and, where the Academy sends email through the platform, the recipient's address and the content of that message are processed by **Resend** in the **United States**. The Canadian leg is the storage; the United States leg is email only.

(a) Adequate protection — POPIA's own conditions, applied to us by contract. We agree that, in respect of personal information received from the Academy, we will uphold principles for

reasonable processing substantially similar to the conditions for lawful processing in Chapter 3 of POPIA, namely:

CONDITION	WHAT WE AGREE TO
Accountability (§8)	We are answerable to the Academy for compliance with this clause, and we do not treat the Academy's obligations as discharged by ours.
Processing limitation (§§9–12)	We process only on the Academy's documented instructions, only so far as is necessary to provide the service, and we do not process for our own purposes.
Purpose specification (§§13–14)	We use the information only for the purposes in §2 of this agreement, and retain it only as §11 provides.
Further processing limitation (§15)	We do not process for any purpose incompatible with the one it was collected for. We do not sell it, and we do not use it to train models.
Information quality (§16)	The Academy controls and corrects its own records directly in the panel, and we do not alter the substance of them.
Openness (§§17–18)	This agreement, Annex A and the privacy policy state what we hold, where it is, and who else touches it. Changes to sub-processors carry 30 days' notice under §7.
Security safeguards (§§19–22)	The measures in Annex B, and the separation between Academies enforced in the database rather than in the application.
Data subject participation (§§23–25)	We assist the Academy in responding to a data subject who asks what is held, or asks for correction or deletion, and the Academy can export or delete its records itself at any time.

(b) Onward transfer — the part §72(1)(a)(ii) specifically requires. We will not further transfer personal information received from the Academy to a third party in a foreign country unless that third party is bound by a law, binding corporate rules or a binding agreement which provides an adequate level of protection meeting the standard in (a) above **and which itself restricts onward transfer on terms substantially similar to this paragraph**. Each sub-processor in Annex A is engaged on written terms imposing obligations no less protective than these, and we remain liable to the Academy for their performance. Adding or replacing a sub-processor carries the notice and objection right in §7.

(c) Breach, for a South African Academy. §21(2) requires us to notify the responsible party **immediately** where there are reasonable grounds to believe personal information has been accessed by an unauthorised person. The 48 hours in §9 of this agreement does not apply here: we notify immediately on becoming aware, and follow with detail as we have it. §22's notification to the Regulator and to data subjects is the Academy's to make, as responsible party, as soon as reasonably possible.

(d) What this clause does not do. It does not create an adequacy finding, and it is not a determination by the Information Regulator. It is the binding agreement route in §72(1)(a), which is the route available to two private parties without one. Whether a United States incorporated provider storing data in a Canadian AWS region is itself subject to PIPEDA is not treated by us as settled, and it bears on how strong the underlying protection is — not on whether this clause is the right instrument.

1. **§35, children.** The Academy carries the lawful-basis obligation. Worth noting for a South African Academy that the prohibition is structured as a ban with exceptions rather than as a consent requirement, which is a stricter starting point than it first reads.

C5 — United States

6 Academies, most of them in Texas.

There is no federal privacy statute of general application. What applies is a stack: a federal children's law, a growing set of state statutes, and — for anything touching schools — student-privacy law. The stack, not any one item, is the schedule.

Roles	Business / **service provider** (California and most state statutes)
Child	Under 13 for COPPA. Several state statutes use under 18 for targeted advertising and sale.
Breach	State-by-state, by statute; several require notification to the state Attorney General

1. COPPA (federal, under 13). The check-in page a child fills in **deliberately does not ask a child for an email address or an age** — name, a slider and a message. That is a design decision made for this rule. Where an Academy enters a child's details, the Academy is the one with the relationship with the family and the one that must have parental consent. Whether we are nonetheless an "operator" for the pages we host, and whether the school-consent route is available to a **private coaching academy — which is not a school** — is the single most important American question for this business.

2. California (CCPA/CPRA). The contract terms a service provider agreement must contain are in §2 of the main body, specifically the prohibitions on retaining, using or disclosing the data for any purpose other than performing the service, on selling or sharing it, and on combining it with other data. We certify our understanding of those restrictions by entering into this agreement. California also has **SOPIPA**, which restricts operators of K-12 school services — relevant if an Academy is a school rather than a club.

3. Texas, where most of our American Academies are. The **Texas Data Privacy and Security Act** imposes its own required processor contract terms, and the **SCOPE Act** addresses minors. Both

need checking against this document rather than assumed to be covered by the Californian wording.

4. Other states. Virginia, Colorado, Connecticut, Utah, Oregon, Montana and a growing list have comprehensive statutes with processor-contract requirements that are similar but not identical. The practical approach is to meet the strictest and apply it everywhere, which is what §2 does.

5. FERPA and state student-privacy law. FERPA binds schools receiving federal funding, which a private coaching academy generally is not. If we ever sell to a school district — New York's Education Law §2-d is the strictest example — that is a different contract entirely, and this one does not cover it.

6. Transfers. The United States imposes no general restriction on personal data leaving the country, so the Canadian store raises no US-side transfer problem. The direction that matters is data arriving *in* the US via Resend, and that is the EEA and UK schedules' problem, not this one's.

C6 — Canada

No Academies today — but this is where the data lives, so the schedule is not hypothetical.

Law	PIPEDA; Quebec's Law 25 for data subjects in Quebec
Regulator	Office of the Privacy Commissioner of Canada; the Commission d'accès à l'information for Quebec
Roles	Organisation / third-party processor
Child	No fixed federal age; Quebec's Law 25 has specific provisions for under-14s

What this schedule adds. PIPEDA holds a transferring organisation accountable for personal information handed to a processor, and expects contractual protection comparable to its own. This agreement is that protection. Storing in Canada does not by itself make PIPEDA apply to a Nigerian or American Academy — but it does mean Canadian law reaches the data at rest, including lawful access requests, which is a fact a European customer will ask about and which belongs in a transfer impact assessment rather than being discovered during one.

C7 — Markets the product is already built for

The platform prices in **16 currencies** and reads in **10 languages** — 16 as of 24 August 2026, when the Qatari riyal joined the list. Every country below is therefore one we could take a signup from tomorrow, which makes each of them a gate rather than a plan. None has an Academy today.

Each row names the specific thing that would bite, so that an Academy in that market can see what applies before it asks.

MARKET	STATUTE	REGULATOR	THE THING THAT WOULD BITE
India (INR)	Digital Personal Data Protection Act 2023	Data Protection Board	**Everyone under 18 is a child**, verifiable parental consent is required, and tracking or behavioural advertising directed at children is prohibited outright. For a platform whose users are mostly minors this is the most demanding regime on this list.
China (zh)	Personal Information Protection Law	Cyberspace Administration of China	Cross-border transfer needs a CAC security assessment, the CAC standard contract, or certification; an offshore processor needs a **domestic representative** and filing. Realistically not servable at this size — say so rather than list China as a market.
UAE (AED)	Federal Decree-Law 45 of 2021, plus separate DIFC and ADGM regimes	UAE Data Office; DIFC and ADGM commissioners	Which of the three regimes applies depends on where the Academy sits, and they are not the same law.
Singapore (SGD)	Personal Data Protection Act 2012	PDPC	We would be a **data intermediary**, with protection and retention obligations directly on us rather than only via contract.
Australia (AUD)	Privacy Act 1988, Australian Privacy Principles	OAIC	**APP 8** makes the Academy accountable for our acts abroad unless it takes reasonable steps; the Notifiable Data Breaches scheme sets the timing.
Kenya (KES)	Data Protection Act 2019	ODPC	**Registration** of data controllers and processors with the ODPC, with thresholds. A registration gate, not a clause.
Ghana (GHS)	Data Protection Act 2012	Data Protection Commission	Registration is broad and is enforced. Another gate.

MARKET	STATUTE	REGULATOR	THE THING THAT WOULD BITE
Egypt (EGP)	Law 151 of 2020	Personal Data Protection Centre	Contemplates **licences and permits**, including for cross-border transfer. Confirm what is actually operative before quoting a price to an Egyptian academy.
Morocco (MAD)	Law 09-08	CNDP	Prior **notification or authorisation** to the CNDP, and authorisation for transfers abroad.
Senegal, Côte d'Ivoire and the CFA franc zone (XOF)	National laws under the ECOWAS Supplementary Act and the AU Malabo Convention	CDP (Senegal), ARTCI (Côte d'Ivoire), and national equivalents	Several require prior declaration. The regional instruments do not remove the national filing.
EEA / UK (EUR, GBP)	See C2, C3		Representative and transfer mechanism, both absent.

C8 — Qatar

One Academy (Abass tennis Academy, Doha). Added 24 August 2026, the day it signed up.

Law	Law No. 13 of 2016 on Protecting Personal Data Privacy (PDPPL)
Regulator	**[counsel to confirm]** — oversight has sat with the Ministry of Transport and Communications; confirm the operative authority before this schedule is signed
Roles	Data controller / data processor
Child	**[counsel to confirm]** — the PDPPL requires a guardian's consent for children's data; the exact age line is deliberately not stated here, because guessing an age onto paper is how a schedule stops being evidence and starts being a liability
Breach	**[counsel to confirm]** — timing and recipient of notification

What this schedule adds.

1. Until counsel fills the three fields above, the honest content of this schedule is the main body §1–§13 plus the statute's name. That thinness is deliberate: a schedule that invents specifics is worse than one that admits the gap, and Annex E already says what a contract cannot do.
2. **Transfers.** The records leave Qatar for Canada and the United States (Annex A). The PDPPL restricts taking personal data out of the country without adequate protection or another

permitted basis; which basis we rely on is **[counsel to confirm]**. This is the same shape of question C1 answers for Nigeria, and it should get that quality of answer before a second Qatari Academy signs — not after.

3. **Governing law unchanged.** Per §13 the contract itself remains under the law of the Federal Republic of Nigeria. This schedule exists because Qatar's own data protection statute applies to Qatari families regardless of what any contract says — writing it down is how everyone can see what is agreed rather than assume it.

Annex E — What this agreement cannot do

Signing a DPA with an Academy does not make us lawful in that Academy's country. These are the obligations that sit on *us*, that no contract supplies, and that in several cases must be complete **before** the first customer in that market is served.

GATE	WHERE	STATUS
NDPC registration	Nigeria	**Granted — NDPC/DCP/14079**, in the name of Sleek&Tech System Ltd since 14 August 2026. Same number as the original grant.
Data Protection Officer	Nigeria	**Appointed and registered with the NDPC**, August 2026
EEA Article 27 representative	European Economic Area	**Not appointed** — blocks the first EEA Academy
UK Article 27 representative	United Kingdom	**Not appointed** — blocks the first UK Academy
EU Standard Contractual Clauses, Modules Two and Three	EEA	**Not executed**
UK IDTA or Addendum	United Kingdom	**Not executed**
Transfer impact assessment	EEA, UK	**Not done**
Article 30(2) processing record	EEA, UK	Partially — Annex A and §§2–3 are the substance, not yet a maintained document
POPIA §72 transfer wording	South Africa	**2 live Academies.** Being relied on today without the drafted wording.
ODPC registration	Kenya	Not started
Data Protection Commission registration	Ghana	Not started
CNDP notification	Morocco	Not started
Licences / permits	Egypt	Not investigated
CAC mechanism and domestic representative	China	Not started; may be out of reach at this size
Country field on the Academy record	Everywhere	**Does not exist.** Blocks operating any of the above per-Academy.
Cyber / professional indemnity insurance	Everywhere	Not in place

Read this table as the answer to "can we operate there". The two rows with live Academies behind them — POPIA transfer wording, and the missing country field — are the ones carrying

actual exposure today. Everything else is a door that is closed rather than a fire that is burning.

Questions about this agreement, or a request for it as a separately signed document, go to info@sleektechsport.com.