Data Protection and Data Sharing Agreement

Between Liberation Academy Ltd (trading as Aperio Profiles) and the Organisation Customer

Version 3, 8 October 2026

Applies to every organisation that accepts it on or after 8 October 2026. For an organisation that accepted an earlier version, this version takes effect 30 days after Aperio gives notice of it under clause 9.4 of version 2.

1. Parties, status and background

1.1 This Agreement is between Liberation Academy Ltd, a company registered in England and Wales (company number 16087057), registered office 20 Wenlock Road, London N1 7GU, ICO registration reference ZB819301, trading as Aperio Profiles ("Aperio"), and the organisation that accepts this Agreement when it sets up its Aperio organisation account, signs an order, or otherwise uses the Aperio organisation platform (the "Customer"). Each is a "party".

1.2 This Agreement governs the parties' data protection responsibilities, and the Customer's use of Aperio Data, for personal data processed through the Aperio platform when the Customer's Workers complete Aperio assessments or screeners funded by the Customer, when the Customer uploads an employee list, and when the Customer uses the Aperio organisation dashboard.

1.3 This Agreement is a complete and binding agreement in its own right. Where the parties have also signed an Aperio Organisation Services Agreement or order form (a "Services Agreement"), this Agreement forms part of it. If the two conflict on a data protection matter or on the Customer's use of Aperio Data, this Agreement prevails.

1.4 The person who accepts this Agreement on the Customer's behalf confirms that they are authorised to bind the Customer. The Customer is bound from the earlier of acceptance and first use of the organisation platform.

2. Definitions

2.1 "Data Protection Legislation" means the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, each as amended or replaced from time to time, including by the Data (Use and Access) Act 2025. "Controller", "processor", "joint controllers", "personal data", "special category data", "data subject", "processing" and "personal data breach" have the meanings given in that legislation.

2.2 "Worker" means any employee, worker, contractor, volunteer or other individual the Customer invites to use Aperio or adds to its employee list.

2.3 "Shared Profile" means the part of a Worker's workplace profile that is shared with the Customer when the Worker completes a Customer-funded Workplace Profile, as described in clause 3.2.1.

2.4 "Aperio Data" means the Shared Profile, any workplace adjustment a Worker chooses to share, any Aggregate Figure, any other personal data, score, profile, figure, report or output the Customer receives through the platform, and anything copied, derived or inferred from any of them.

2.5 "Aggregate Figures" means the anonymous, organisation-wide figures described in clause 3.4.

2.6 "Authorised User" means an individual the Customer has given access to the organisation dashboard in a role the platform provides (administrator, manager, resourcer or viewer).

2.7 "Prohibited Use" means any use of Aperio Data that clause 4 does not permit.

3. Roles of the parties

The parties process personal data in distinct capacities. This clause allocates them. The detail is in Schedules 1 and 2.

3.1 Aperio as controller

3.1.1 Aperio is the sole controller for: each individual's Aperio account; assessment and screener responses; executive-function, personality and any neurodivergence screening results; the special category (health) data these produce; the consent relationship with the individual; and the retention of that data. Aperio determines the purposes and means of this processing and gives each individual their own account and results.

3.1.2 Aperio's lawful basis for the special category data is the individual's explicit consent under Article 9(2)(a) UK GDPR. The Customer does not instruct, and is not responsible for, this processing, and has no right to receive this data.

3.2 Aperio and the Customer as joint controllers of the Shared Profile

3.2.1 The Shared Profile consists of the Worker's name, work email address and job title, their five OCEAN personality scores and the working-style role derived from them, their stated work arrangement, any workplace adjustment the Worker chooses to share and, where the Worker separately chooses to disclose it, the area a shared adjustment relates to. For the Shared Profile, Aperio and the Customer are joint controllers within the meaning of Article 26 UK GDPR.

3.2.2 Aperio determines what is collected, how it is scored, what is shown to the Customer and the technical means. The Customer determines how it uses the Shared Profile within its organisation, strictly within the limits of clause 4. Schedule 2 sets out each party's responsibilities. The essence of the arrangement is made available to data subjects in Aperio's privacy notice. A data subject may exercise their rights against either party.

3.2.3 Sharing the baseline part of the Shared Profile (name, work email, job title, personality scores, working-style role and work arrangement) with the Customer is the purpose of a Customer-funded Workplace Profile. It contains no special category data. Aperio shares it on the basis of legitimate interests (Article 6(1)(f) UK GDPR) and not on the basis of the Worker's consent. Before a Worker starts, Aperio shows them exactly what the Customer will and will not see, and the Worker may decline. After completion the Worker may choose, in their Aperio account, to restrict the Shared Profile to the Customer's administrators (HR) only.

3.2.4 A workplace adjustment, and the area it relates to, are shared only where the Worker makes a separate, explicit choice to share them, and the Worker may withdraw either at any time. Neither is part of the baseline described in clause 3.2.3.

3.2.5 The Customer is responsible for its own lawful basis for its use of the Shared Profile and of any shared adjustment, including any condition it needs under Article 9 UK GDPR and Schedule 1 to the Data Protection Act 2018. The Customer will not rely on a Worker's consent as its lawful basis for using the baseline Shared Profile.

3.3 Aperio as processor

3.3.1 Where Aperio processes personal data solely on the Customer's documented instruction and not for any purpose Aperio itself determines, Aperio acts as the Customer's processor. This covers: storing the employee list the Customer uploads (name, work email, job role, team and manager); sending account invitations and Workplace Profile access codes to the recipients the Customer names; and actioning a Customer request in respect of a Worker, such as recording a leaver. Aperio processes such data only on the Customer's documented instructions, given through the dashboard or in writing, unless the law requires otherwise, in which case Aperio will tell the Customer first where the law permits. Aperio will tell the Customer if, in its opinion, an instruction infringes the Data Protection Legislation.

3.3.2 For that processing Aperio will: ensure that persons authorised to process the data are bound by confidentiality; implement the measures in clause 7 and Schedule 3; engage sub-processors only under clause 9; assist the Customer with data subject requests and with its obligations under Articles 32 to 36 UK GDPR, taking into account the nature of the processing and the information available to Aperio; delete or return the data under clause 10.3; and make available the information needed to demonstrate compliance under clause 11. This clause 3.3 and Schedule 1 are the contract required by Article 28(3) UK GDPR.

3.3.3 The Customer confirms that it has a lawful basis to give Aperio the employee list and that it has told its Workers that it will do so.

3.4 Anonymous aggregate figures

3.4.1 ADHD, autism and bias screeners are requested anonymously. The Customer is never told who requested or completed a screener, which screener an individual took, or any individual result. The Customer receives only organisation-wide figures: how many screeners were completed and, for the ADHD and autism screeners, how many people scored in the high range. Aperio suppresses a figure unless at least five people fall inside the group it counts and at least five fall outside it.

3.4.2 Aggregate Figures are provided as anonymous information. If the Customer is nonetheless able to link a figure to an individual, it must treat that information as special category data, must not use, record or disclose it, and must tell Aperio within five working days.

4. Permitted use and use restrictions

The restrictions in this clause are a condition of the Customer's access to the Aperio platform and to Aperio Data. They keep the processing lawful and protect data subjects. Each of them is a material term of this Agreement.

4.1 **Permitted purposes.** The Customer will use Aperio Data only to understand how individuals work best, to manage and support them, to compose and balance teams, and to identify and provide reasonable adjustments and support (the "Permitted Purposes"). It will not use Aperio Data for any other purpose.

4.2 **No decisions about an individual.** The Customer will not use any individual's Aperio Data (including their personality scores, working-style role, work arrangement, participation or non-

participation, shared adjustments, or anything inferred from them) as a basis for, or as a factor in, any decision about that individual concerning recruitment, selection, promotion, pay, bonus, grading, disciplinary action, performance management, capability procedures, redundancy selection, redeployment, dismissal, references, or any other decision that is adverse to that individual. It will not use Aperio Data to make, or to materially inform, any decision based solely on automated processing that produces legal or similarly significant effects.

4.3 **No candidate assessment.** The Customer will not use Aperio to assess, screen, rank or select job applicants or candidates (including internal candidates for a specific vacancy), and will not ask an applicant or candidate to complete any Aperio assessment or screener. The Workplace Profile asks about matters that touch on health, and section 60 of the Equality Act 2010 restricts asking applicants about health before an offer of work. Aperio has not been validated as a selection tool.

4.4 **Team-level planning.** The Customer may use the overall balance of working styles across an existing team when it plans what a new role needs. If it does:

(a) it will use team-level information only, and never an individual's Aperio Data;

(b) the Customer alone decides how to recruit, and alone is responsible for making sure that its recruitment arrangements, criteria and decisions are lawful, including under the Equality Act 2010 and in particular the provisions on direct and indirect discrimination, discrimination arising from disability and the duty to make reasonable adjustments;

(c) Aperio gives no advice, assurance or warranty that any recruitment criterion based on working style is lawful, valid or fair, and the Customer does not rely on Aperio for that; and

(d) the Customer will take its own legal advice before building working style into a selection process.

4.5 **Voluntary participation and no detriment.** Participation is voluntary. The Customer will not require a Worker to take part; will not make participation a condition of any role, contract, handbook, policy or onboarding process; will not ask a Worker why they declined or did not complete an assessment; will not record non-participation on any personnel file; and will not treat a Worker who declines, who does not complete, or who withdraws anything they have shared, less favourably in any respect. Workers who have no profile remain fully eligible for any team, project or opportunity.

4.6 **Not clinical information.** Aperio assessments and screeners are not diagnostic tools and do not provide a diagnosis. The Customer will not describe or treat any Aperio output, including any Aggregate Figure, as a diagnosis, a medical opinion or evidence that any individual has or does not have any condition, and will not use Aperio Data in place of occupational health or clinical advice where that advice is needed.

4.7 **Least-privilege access.** The Customer will give dashboard access only to Authorised Users who need it for the Permitted Purposes, in the most limited role that meets that need; will respect a Worker's choice to restrict their Shared Profile to administrators (HR) only, and will not ask a Worker to change that choice; will make sure each Authorised User has their own login and does not share it; will keep access under review and remove it promptly when it is no longer needed, including when an Authorised User leaves or changes role; and will keep dashboard credentials secure.

4.8 **No re-identification.** The Customer will not attempt to identify any individual from Aggregate Figures or other anonymous information; will not combine data, filter repeatedly, or time requests in order to defeat the small-number suppression built into the dashboard; and will not

ask a Worker, or anyone else, whether a Worker has requested or taken a screener, or what their result was.

4.9 **No onward disclosure.** The Customer will not sell, license or disclose Aperio Data to any third party, including recruitment agencies, other employers, prospective employers and referees, except to its own professional advisers under a duty of confidence, or where the law requires disclosure. Any copy the Customer makes of Aperio Data, in any system, remains Aperio Data and remains subject to this Agreement.

4.10 **No re-use in other systems.** The Customer will not input Aperio Data into any other automated system, including any artificial intelligence, analytics, people-scoring or workforce-management tool, except for the Permitted Purposes and subject to clause 4.2, and will not use Aperio Data to train, test or build any model or product.

4.11 **Equality and fairness.** The Customer will comply with the Equality Act 2010, including its duty to make reasonable adjustments, and will not use Aperio Data in a way that amounts to direct or indirect discrimination, discrimination arising from disability, harassment or victimisation.

4.12 **Its own obligations.** As controller or joint controller of the data it holds, the Customer will maintain its own lawful basis for its use of Aperio Data, give its Workers the information it is responsible for under Schedule 2, keep its records of processing, keep the data secure, and carry out a data protection impact assessment and, where appropriate, an equality impact assessment before deploying the platform, keeping both under review.

4.13 **Reporting misuse.** The Customer will tell Aperio in writing within five working days of becoming aware of any actual or suspected Prohibited Use, by any person, and will take prompt steps to stop it and to prevent it recurring.

4.14 **Aperio's remedies.** If Aperio reasonably believes that the Customer or an Authorised User has engaged in a Prohibited Use, Aperio may, without liability, suspend the Customer's access to Aperio Data, or to the dashboard, until the matter is resolved to Aperio's reasonable satisfaction, and may terminate this Agreement under clause 13.2. Aperio may tell affected Workers what has happened where it considers that necessary to protect them.

5. Data subjects' rights and complaints

5.1 Aperio gives each individual self-service access, data export and erasure-request tooling in their Aperio account, and honours withdrawal of any consent and of anything the individual has chosen to share. Aperio handles rights requests relating to the data for which it is the sole controller.

5.2 For the Shared Profile, requests may be made to either party. Schedule 2 sets out which party leads on each right. A party that receives a request for which the other leads will pass it to the other within five working days. Each party will give the other the assistance and information it reasonably asks for within five working days, so the request can be met within the statutory time limit.

5.3 Aperio leads on any objection under Article 21 UK GDPR to the sharing of the baseline Shared Profile. Aperio will assess each objection individually, and the Customer will give Aperio, within five working days of being asked, any information Aperio reasonably needs to do so. If Aperio upholds an objection, it will withdraw the Shared Profile from the Customer's dashboard, and the Customer will delete any copy it holds within 30 days and confirm that it has done so.

5.4 Each party will handle complaints about its own processing in line with section 164A of the Data Protection Act 2018, including acknowledging a complaint within 30 days of receiving it. A party that receives a complaint about the other's processing will pass it to the other within five working days.

5.5 Where Aperio acts as processor, it will assist the Customer by appropriate technical and organisational measures, so far as possible, to respond to data subject requests.

5.6 When the Customer records that a Worker has left, that Worker's Shared Profile and shared adjustments are withdrawn from every Customer-facing view. The individual's own account and report are unaffected.

6. Information to Workers

6.1 Aperio provides the transparency information for the assessment, the health data and Aperio's own processing, including the employer disclosure notice each Worker is shown before starting a Customer-funded profile. The Customer will tell its Workers, in its own privacy information, how it uses Aperio Data within its organisation, and that it does so within the restrictions in clause 4.

6.2 Neither party will say anything to Workers about Aperio, or about how Aperio Data is used, that contradicts this Agreement or Aperio's privacy notice. In particular, the Customer will not tell any Worker that participation is compulsory or expected.

7. Security

7.1 Each party will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the special category nature of much of the data (Article 32 UK GDPR). Aperio's measures are summarised in Part A of Schedule 3. The Customer will, as a minimum, apply the measures in Part B of Schedule 3.

7.2 Each party will ensure that persons authorised to process the personal data are bound by confidentiality.

8. Personal data breach

8.1 A party that becomes aware of a personal data breach affecting personal data covered by this Agreement, including the compromise of an Authorised User's login, will notify the other without undue delay and in any event within 48 hours of becoming aware, with the information the other reasonably needs to meet its own obligations under Articles 33 and 34 UK GDPR, and will update that information as it becomes available.

8.2 The parties will co-operate to investigate, contain, mitigate and remediate the breach, and will each keep a record of it. For the Shared Profile, the party in whose systems or organisation the breach occurred leads on notifying the Information Commissioner and affected individuals, unless the parties agree otherwise. Neither party will name the other in any public statement about a breach without first consulting it, unless the law requires otherwise.

9. Sub-processors and international transfers

9.1 The Customer gives Aperio general written authorisation to engage the sub-processors listed in Schedule 4. Aperio imposes data protection terms on each that are no less protective than this Agreement, and remains responsible for their performance. Aperio will give the Customer at least

30 days' notice of any intended addition or replacement and the Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Customer may end this Agreement, and any Services Agreement, on written notice.

9.2 Aperio's database is hosted in the United Kingdom (Supabase, on Amazon Web Services in London). Some sub-processors process personal data outside the United Kingdom, as set out in Schedule 4. Any such transfer is made under a mechanism permitted by the Data Protection Legislation, such as UK adequacy regulations (including the UK Extension to the EU-US Data Privacy Framework for a certified recipient), the UK International Data Transfer Agreement, or the UK Addendum to the EU Standard Contractual Clauses.

9.3 The Customer will not transfer Aperio Data outside the United Kingdom except under such a mechanism.

10. Retention and deletion

10.1 Aperio retains personal data in accordance with its published retention schedule, which sets a period for each category of data. At the date of this version: raw assessment answers are deleted or anonymised about 90 days after the report is produced; results are kept while the individual's Aperio account is active and, where the individual has no account, are deleted 24 months after their last activity; access codes and session tokens are kept for up to 12 months; audit and access logs for up to 18 months; and consent records, records of a workplace adjustment shared with the Customer, and payment records for up to six years.

10.2 The Customer will keep any copy it makes of Aperio Data only for as long as it needs it for the Permitted Purposes, and will delete any copy relating to a Worker within 30 days after that Worker leaves, except where the law requires the Customer to keep it (for example, evidence of a reasonable adjustment), in which case it will keep only what is required, for as long as is required.

10.3 When this Agreement ends, Aperio will, at the Customer's choice, delete or return the personal data it processes as the Customer's processor, except to the extent the law requires Aperio to keep it or Aperio is entitled to keep it as controller. The Customer will delete all Aperio Data it holds within 30 days, except as clause 10.2 allows, and will confirm in writing that it has done so if Aperio asks. Individuals keep their own accounts and reports.

11. Records, compliance checks and audit

11.1 Aperio will make available the information necessary to demonstrate compliance with this Agreement and will allow for and contribute to audits, including inspections, conducted by the Customer or an auditor it mandates, no more than once in any 12 months (or following a personal data breach), on at least 30 days' notice, during business hours and subject to confidentiality. An audit will not give access to any individual's special category data or to another customer's data.

11.2 No more than once in any 12 months, or at any time if Aperio reasonably suspects a Prohibited Use, Aperio may ask the Customer to confirm in writing, within 30 days, that it has complied with clause 4, and to give reasonable supporting information, including a list of its Authorised Users and their roles.

12. Liability and indemnity

12.1 **Indemnity.** The Customer will indemnify Aperio against all losses, damages, compensation, settlements, costs and reasonable legal and professional expenses, and, to the extent the law permits, fines and penalties, that Aperio incurs as a result of any claim, complaint, tribunal or court proceeding, or regulatory action brought by a Worker, an applicant for work, a regulator or any other third party, to the extent it arises from: (a) the Customer's or an Authorised User's breach of clause 4; (b) any recruitment, selection or other employment decision made by the Customer; or (c) the Customer's breach of the Data Protection Legislation. Nothing in this clause makes the Customer responsible for a claim to the extent it results from Aperio's own breach of this Agreement or of the Data Protection Legislation.

12.2 **Conduct of claims.** Aperio will tell the Customer promptly of any claim covered by clause 12.1, will not settle it without consulting the Customer, and will give the Customer reasonable assistance at the Customer's cost. Aperio may conduct its own defence.

12.3 **Data subject compensation between the parties.** Where both parties are liable to a data subject for the same damage, each is entitled to recover from the other the part of any compensation it has paid that corresponds to the other's share of responsibility for the damage, in accordance with Article 82(5) UK GDPR.

12.4 **Aperio's limit.** Subject to clause 12.6, Aperio's total liability to the Customer arising out of or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is limited in each period of 12 months to the greater of the fees the Customer paid to Aperio in the 12 months before the event giving rise to the liability and £1,500. Where a Services Agreement is in force, the limit in that agreement applies instead if it is higher.

12.5 **Excluded losses.** Subject to clause 12.6, Aperio is not liable for any loss of profit, revenue, business, goodwill or anticipated savings, or for any indirect or consequential loss.

12.6 **Unlimited matters.** Nothing in this Agreement limits or excludes liability for death or personal injury caused by negligence, for fraud or fraudulent misrepresentation, or for any other liability that cannot lawfully be limited or excluded. The limits in clauses 12.4 and 12.5 do not apply to the Customer's liability under clause 12.1. Nothing in this Agreement limits a data subject's rights or a regulator's powers against either party.

13. Term, suspension and termination

13.1 This Agreement continues while the Customer has an Aperio organisation account and for as long as either party processes personal data covered by it.

13.2 Aperio may terminate this Agreement, and close the Customer's organisation account, immediately on written notice if the Customer commits a material breach of clause 4, or any other material breach that is not remedied within 14 days of written notice. Each party may terminate on written notice if the other becomes insolvent.

13.3 Clauses 3.4.2, 4.2, 4.3, 4.6, 4.8, 4.9, 4.10, 5.3, 10, 12 and 15 continue after this Agreement ends for as long as the Customer holds any Aperio Data, and clause 12 continues indefinitely in respect of matters arising before then.

14. Changes

14.1 Aperio may update this Agreement to reflect changes in the law, in regulatory guidance or in the platform. Aperio will give the Customer at least 30 days' notice of any material change, by email to the Customer's account administrator and in the dashboard.

14.2 The updated Agreement applies from the end of the notice period. If the Customer does not accept a material change, it may end this Agreement by written notice before the change takes effect. Continued use of the platform after the change takes effect is acceptance of it. A change required by law may take effect sooner where the law requires.

15. General

15.1 **Notices.** Notices under this Agreement must be in writing and may be sent by email: to Aperio at enquiries@liberationacademy.co.uk, and to the Customer at the email address of its account administrator. A notice sent by email is received on the next working day after sending.

15.2 **Third parties.** No one other than the parties has any right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement. This does not affect any right a data subject has under the Data Protection Legislation.

15.3 **Severance.** If any provision of this Agreement is found invalid or unenforceable, it will apply with the minimum modification needed to make it valid and enforceable, and the rest of this Agreement is unaffected.

15.4 **Assignment.** The Customer may not assign or transfer this Agreement without Aperio's written consent. Aperio may assign it to a successor to the Aperio business that agrees to be bound by it.

15.5 **Waiver.** A failure or delay in exercising a right is not a waiver of it.

15.6 **Order of precedence.** If there is a conflict, the order of precedence is: the body of this Agreement, then its Schedules, then any Services Agreement, then any other terms.

15.7 **Law and jurisdiction.** This Agreement and any dispute or claim arising out of or in connection with it are governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

Schedule 1: Details of processing

Item	Detail
Subject matter	Provision of workplace profiling and screening assessments and the associated organisation dashboard.
Duration	The term of this Agreement, plus the periods in the retention schedule.
Nature	Collection, storage, organisation, automated scoring, retrieval, disclosure to the data subject and, for the Shared Profile, to the Customer, and deletion.
Purpose	Understanding how individuals work best, composing and supporting teams, and identifying reasonable adjustments and support.
Data types	Identifiers (name, work email, job title, team, manager); assessment responses; executive-function and OCEAN personality scores; working-style role; work arrangement; where the individual opts in, neurodivergence screening results and any diagnoses they disclose (special category health data, never shared with the Customer); shared adjustments and, where disclosed, the area they relate to.
Data subjects	The Customer's Workers who are on the employee list or who choose to complete an assessment, and the Customer's Authorised Users.
Processor processing (clause 3.3)	Storage of the employee list; sending invitations and access codes to recipients the Customer names; actioning Customer requests such as recording a leaver.

Schedule 2: Joint controller allocation (Shared Profile)

For the Shared Profile, the parties allocate responsibility as follows. The essence of this arrangement is made available to data subjects in Aperio's privacy notice.

Responsibility	Lead party
Transparency information about the assessment, the health data, Aperio's processing and what is shared (Articles 13 and 14), including the employer disclosure notice	Aperio
Transparency about the Customer's own use of the Shared Profile within its organisation	Customer
Lawful basis for sharing the baseline Shared Profile with the Customer	Aperio: legitimate interests (Article 6(1)(f)). Not based on consent.
Lawful basis for sharing a workplace adjustment, and the area it relates to	Aperio: the Worker's explicit consent (Articles 6(1)(a) and 9(2)(a)), withdrawable at any time
Lawful basis for the Customer's own use of the Shared Profile and any shared adjustment	Customer
Access, portability, rectification, erasure and withdrawal for the platform record	Aperio (Customer assists)
Objections under Article 21 to the baseline sharing	Aperio (Customer assists and deletes copies if an objection is upheld)

Responsibility	Lead party
Access, rectification and erasure for copies the Customer has taken or exported	Customer
Complaints about the platform and Aperio's processing (DPA 2018 s.164A)	Aperio
Complaints about the Customer's use of Aperio Data	Customer
Personal data breach in Aperio's systems	Aperio
Personal data breach in the Customer's systems or arising from an Authorised User's login	Customer
Single point of contact for data subjects	Aperio (enquiries@liberationacademy.co.uk)

Schedule 3: Security measures

Part A: Aperio's measures (summary)

- Access to personal data is role-scoped and enforced server-side, with deny-by-default database policies and tenant isolation between customers.
- Special category data is minimised before it reaches the Customer: an individual's sex, executive-function scores, screening results, diagnoses and answers are never shown to the Customer, and Aggregate Figures use small-number suppression.
- Respondent-only credentials protect a person's screening record. Secrets are stored only as keyed hashes and are kept out of URLs.
- Transport security (HTTPS and HSTS), security response headers, and encryption in transit and at rest through the hosting providers.
- Access to special category data is logged, administrative actions are recorded, retention periods are enforced by automated daily jobs, and personal data breach procedures are in place.

This is a summary. The full technical and organisational measures are maintained separately and are available on request.

Part B: the Customer's minimum measures

- Each Authorised User has their own login, which is not shared, and a strong, unique password.
- Dashboard access is limited to the roles that need it, reviewed at least every six months, and removed promptly when an Authorised User leaves or changes role.
- Aperio Data is not downloaded, printed or copied except where needed for the Permitted Purposes, and any copy is stored securely with access limited to those who need it.
- Authorised Users are told about the restrictions in clause 4 before they are given access.
- Workers who leave are recorded as leavers in the dashboard promptly.

Schedule 4: Sub-processors

Sub-processor	Purpose	Location and safeguard
Supabase	Database, authentication and storage	United Kingdom (AWS London, eu-west-2)
Vercel	Application hosting and content delivery	Application functions run in London. Requests may be routed through Vercel's global network; Vercel is a US company, and any transfer is safeguarded as clause 9.2 describes
Resend	Transactional email delivery	Email is sent from Resend's EU region. Resend is a US company, so limited support access may occur in the United States, safeguarded as clause 9.2 describes
Stripe	Payment processing. Aperio never sees or stores card details	United States, safeguarded as clause 9.2 describes
Anthropic	AI model behind the Live Help assistant on Aperio's websites. Only what a person types into the assistant is sent; no assessment, screener or Shared Profile data is sent. Anthropic does not use the data to train its models and deletes it within 30 days, unless a message is flagged under its usage policy or the law requires longer retention	United States, safeguarded by the UK Addendum to the EU Standard Contractual Clauses

Acceptance

The Customer accepts this Agreement electronically when its authorised administrator ticks acceptance in the Aperio dashboard, or by first use of the organisation platform. Aperio records the version accepted, the date and time, and the person who accepted. A countersigned copy is available on request.

Signed for and on behalf of Liberation Academy Ltd (Aperio Profiles):

Signature: _____ Date: _____

Name and role: _____

Signed for and on behalf of the Customer:

Signature: _____ Date: _____

Name and role: _____