



Data Protection and Data Sharing Agreement

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

Version 2, 17 September 2026

1. Parties 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 or signs an order (the "Customer"). Each is a "party".
- 1.2** It governs the parties' data protection responsibilities for personal data processed through the Aperio platform when the Customer's workers complete Aperio assessments or screeners funded by the Customer, and when the Customer uploads an employee list. It forms part of the Aperio Organisation Services Agreement between the parties (the "Services Agreement"). If the two conflict on a data protection matter, this Agreement prevails.
- 1.3** "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. "Controller", "processor", "joint controllers", "personal data", "special category data", "data subject", "processing" and "personal data breach" have the meanings given in that legislation. "Worker" means any employee, worker, contractor or other individual the Customer invites to use Aperio. "Aperio Data" means any personal data, score, profile, adjustment, figure or other output the Customer receives through the platform, and anything inferred from it.

2. Roles of the parties

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

2.1 Aperio as controller

- 2.1.1** Aperio is the 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, sets the consent model, and gives each individual their own account and results.
- 2.1.2** 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.

2.2 Aperio and the Customer as joint controllers

- 2.2.1** For the workplace profile that is shared with the Customer when an individual completes a Customer-funded Workplace Profile (the individual's name, work email and job title, their five OCEAN personality scores and the working-style role derived from them, their stated work arrangement, any workplace adjustments the individual chooses to share and, where the individual separately chooses to disclose it, the area a shared adjustment relates to), Aperio and the Customer are joint controllers within the meaning of Article 26 UK GDPR.
- 2.2.2** 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, within the limits of clause 3. Schedule 2 sets out each party's responsibilities, in particular for data subjects' rights and for the information required by Articles 13 and 14. The essence of that arrangement is made available to data subjects in Aperio's privacy notice. Regardless of this allocation, a data subject may exercise their rights against either party.

2.3 Aperio as processor

- 2.3.1** 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 marking a leaver. Clauses 5 to 9 and Schedules 3 and 4 apply to that processing. 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.
- 2.3.2** The Customer confirms it has a lawful basis to give Aperio the employee list and has told its Workers that it will do so.

2.4 Anonymous aggregate figures

- 2.4.1** 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. Where more than 50 people have completed an assessment, the Customer may also see an anonymous, organisation-wide breakdown by sex, which is subject to stricter suppression.
- 2.4.2** These 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 it, and must tell Aperio without delay.

3. The Customer's obligations and use restrictions

These restrictions are a condition of using the Aperio platform. They keep the processing lawful and protect data subjects. The Customer's compliance with them is material to this Agreement and to the Services Agreement.

- 3.1 Purpose limitation.** The Customer will use the shared workplace profile and any shared adjustments 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. It will not use them for any incompatible purpose.
- 3.2 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 any decision about that individual concerning recruitment, selection, promotion, pay, disciplinary action, performance management, redundancy or dismissal, or for any other decision that is adverse to that individual. It will not use Aperio Data to make or materially inform any decision producing legal or similarly significant effects by automated means.
- 3.3 No candidate assessment.** The Customer will not use Aperio to assess, screen, rank or select job applicants or candidates, 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.
- 3.4 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)** 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;
 - (b)** 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
 - (c)** the Customer will take its own legal advice before building working style into a selection process.
- 3.5 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 or onboarding process, and will not treat a Worker who declines, or who later withdraws consent, less favourably in any respect. Workers who have no profile remain fully eligible for any team, project or opportunity.
- 3.6 Least-privilege access.** The Customer will restrict access to Aperio Data to the roles that need it (its dashboard administrators and, where the Worker has chosen to share with them, the Worker's line manager), keep access under review, remove it when it is no longer needed, and keep dashboard credentials secure.
- 3.7 No re-identification.** The Customer will not attempt to identify any individual from aggregate or anonymous figures, will not combine data to defeat the small-number suppression built into the dashboard, and will not ask a Worker whether they have requested or taken a screener.
- 3.8 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.

- 3.9** Its own obligations. As controller or joint controller of the data it holds, the Customer will maintain its own lawful basis for its use, give its Workers the information it is responsible for under Schedule 2, keep the data secure, and carry out a data protection impact assessment and, where appropriate, an equality impact assessment before deploying the platform.
- 3.10** Responsibility and indemnity. The Customer is responsible for how it and its users use Aperio Data. The Customer will indemnify Aperio against all losses, damages, fines, costs and reasonable legal expenses Aperio incurs as a result of any claim, complaint or regulatory action brought by a Worker, an applicant for work, a regulator or any other third party that arises from the Customer's breach of this clause 3, or from any recruitment, selection or other employment decision made by the Customer. 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.

4. Data subjects' rights

- 4.1** Aperio gives each individual self-service access, data export and erasure-request tooling in their Aperio account, and honours withdrawal of consent and of anything the individual has shared. Aperio handles rights requests relating to the data for which it is controller.
- 4.2** For the jointly controlled workplace profile, requests may be made to either party. Schedule 2 sets out which party leads on each right. Each party will assist the other without undue delay, and in any event within five working days of being asked, so the request can be met within the statutory time limit.
- 4.3** 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.
- 4.4** When the Customer marks a Worker as having left, that Worker's profile and shared adjustments are withdrawn from every Customer-facing view. The individual's own account and report are unaffected.

5. Security

- 5.1** 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). Aperio's measures are summarised in Schedule 3.
- 5.2** Each party will ensure that persons authorised to process the personal data are bound by confidentiality.

6. Personal data breach

- 6.1** A party that becomes aware of a personal data breach affecting personal data covered by this Agreement 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.
- 6.2** The parties will co-operate to investigate, mitigate and remediate the breach, and will each keep a record of it. For the jointly controlled workplace 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.

7. Sub-processors and international transfers

- 7.1** The Customer authorises Aperio 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 the Services Agreement on written notice.
- 7.2** Personal data is stored in the United Kingdom (Supabase, hosted 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, for example the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment.

8. Retention and deletion

- 8.1** Personal data is retained in accordance with Aperio's 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.
- 8.2** On termination of the Services Agreement, 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. Individuals keep their own accounts and reports.

9. Audit, liability, term and governing law

- 9.1** 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 and subject to confidentiality. An audit will not give access to any individual's special category data.
- 9.2** Each party is responsible for the processing it carries out and for its own compliance with the Data Protection Legislation. Subject to clause 3.10, liability between the parties is governed by the Services Agreement. Nothing in this Agreement limits a data subject's rights or a regulator's powers against either party. Neither party excludes liability that cannot lawfully be excluded.
- 9.3** This Agreement takes effect when the Customer accepts it, including by ticking acceptance in the Aperio dashboard, or begins using the platform, whichever is first. It continues while the Services Agreement is in force and for as long as either party processes personal data

covered by it. Clauses 3.2, 3.3, 3.7 and 3.10 continue after it ends for as long as the Customer holds any Aperio Data.

9.4 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.

9.5 This Agreement is 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 employer dashboard.
Duration	The term of the Services Agreement, plus the periods in the retention schedule.
Nature	Collection, storage, organisation, automated scoring, retrieval, disclosure to the data subject and (where the data subject chooses) 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); 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.

Schedule 2: Joint controller allocation (workplace profile)

For the jointly controlled workplace profile, the parties allocate responsibility as follows. The essence of this arrangement is made available to data subjects.

Responsibility	Lead party
Transparency information about the assessment, health data and Aperio's processing (Articles 13 and 14)	Aperio
Transparency about the Customer's own use of the profile within the organisation	Customer
Access, portability, rectification, erasure and withdrawal for the platform record	Aperio (Customer assists)
Access, rectification and erasure for copies the Customer has taken or exported	Customer

Responsibility	Lead party
Single point of contact for data subjects	Aperio (enquiries@liberationacademy.co.uk)
Lawful basis for the sharing	Aperio: the individual's agreement recorded at the employer disclosure notice, and Article 9(2)(a) explicit consent for any health-related element the individual chooses to share. Customer: its own basis for its use.

Schedule 3: Aperio's security 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, encryption in transit and at rest through the hosting providers, and reputable managed infrastructure 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.

Schedule 4: Sub-processors

Sub-processor	Purpose	Location
Supabase	Database, authentication and storage	United Kingdom (AWS London, eu-west-2)
Vercel	Application hosting and edge network	Functions may execute outside the UK (safeguarded)
Resend	Transactional email delivery	United States (safeguarded)
Stripe	Payment processing. Aperio never sees or stores card details	United States (safeguarded)

Sub-processor	Purpose	Location
OpenAI	Scoring of free-text answers in the bias screener only. No Workplace Profile, ADHD or autism data is sent. OpenAI does not use API data to train its models. It may retain inputs and outputs for up to 30 days for abuse monitoring, unless the law requires longer. Aperio deletes the free-text answers from its own systems once the individual's results email is sent	United States (safeguarded)

Acceptance. The Customer accepts this Agreement electronically when its authorised administrator ticks acceptance in the Aperio dashboard. Aperio records the version accepted, the date and time, and the person who accepted. A signed copy is available on request.

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

Signed for and on behalf of the Customer: _____ Name and role: _____
Date: _____