

# GDPR Compliance Statement

*ProvisionIQ Ltd — Our Commitment to Data Protection*

|                    |                                                         |
|--------------------|---------------------------------------------------------|
| <b>Document</b>    | GDPR Compliance Statement                               |
| <b>Version</b>     | 1.0                                                     |
| <b>Date</b>        | 22 May 2026                                             |
| <b>Audience</b>    | Schools, LAs, parents, investors, and regulatory bodies |
| <b>Legal basis</b> | UK GDPR (retained EU law) and Data Protection Act 2018  |

## Our Commitment

ProvisionIQ Ltd is built on a foundation of data protection by design and by default. We process some of the most sensitive personal data in the UK education system — the health, educational, and safeguarding records of children with special educational needs. We take that responsibility with the seriousness it demands.

This statement summarises our GDPR compliance position. It is not a substitute for our full Privacy Policy, Data Processor Addendum, or Data Retention Policy.

## 1. Our Role Under UK GDPR

|                                                              |                                                                              |
|--------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>Processing Context</b>                                    | <b>Our Role</b>                                                              |
| <b>Pupil personal data held on behalf of schools and LAs</b> | Data Processor — we process only on the Controller's documented instructions |
| <b>Account data for our own users (staff, admins)</b>        | Data Controller — we determine the purpose and means of processing           |
| <b>Marketing and website data</b>                            | Data Controller                                                              |
| <b>Our own employee and contractor data</b>                  | Data Controller                                                              |

As Data Processor, ProvisionIQ does not determine why or how pupil data is processed — that is the school's or LA's responsibility as Data Controller. We provide the technical infrastructure and process data only as instructed.

## 2. Our Six Data Protection Principles

| Article 5 Principle                                      | How ProvisionIQ Complies                                                                                                                                                                                        |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Lawfulness, fairness, transparency (Art. 5(1)(a))</b> | We publish a clear Privacy Policy. We process only on a documented lawful basis. We never use data in ways that would surprise or harm data subjects.                                                           |
| <b>Purpose limitation (Art. 5(1)(b))</b>                 | Data is used only for the specific purposes for which it was collected. Pupil data is never used for advertising, AI training, or any commercial purpose beyond delivering our service.                         |
| <b>Data minimisation (Art. 5(1)(c))</b>                  | We collect and hold only the data genuinely necessary. Fields are configurable — schools set what is mandatory. We do not require schools to complete fields that are unnecessary for their provision planning. |
| <b>Accuracy (Art. 5(1)(d))</b>                           | Schools can update and correct data at any time. Version control means historical records are preserved. We provide tools for schools to fulfil data subject rectification requests.                            |
| <b>Storage limitation (Art. 5(1)(e))</b>                 | We retain data only as long as necessary. Our Data Retention Policy specifies exact periods for every data category. Automated deletion runs at end of retention period.                                        |
| <b>Integrity and confidentiality (Art. 5(1)(f))</b>      | AES-256 encryption at rest. TLS 1.3 in transit. RBAC. MFA. Immutable audit logs. CREST pen testing. ISO 27001 certified. Cyber Essentials Plus certified.                                                       |

## 3. Lawful Bases

The lawful bases we rely on as Data Controller are: Contract (Art. 6(1)(b)) for user account and service delivery processing; Legitimate Interests (Art. 6(1)(f)) for security, analytics, and relevant B2B marketing; Legal Obligation (Art. 6(1)(c)) for tax and regulatory requirements; and Consent (Art. 6(1)(a)) for any opt-in marketing.

For special category data (including health data in ISP records), we rely on Substantial Public Interest — Education and Training (DPA 2018, Schedule 1, para. 35) where we are acting as Processor on behalf of a school.

## 4. Rights of Data Subjects

ProvisionIQ supports all UK GDPR data subject rights for data we control, and provides technical assistance to Data Controllers handling rights requests for data we process on their behalf. Rights include: Access (SAR), Rectification, Erasure, Restriction, Portability, and Right to Object. See our Privacy Policy and SAR Process for full details.

## 5. Sub-Processors and International Transfers

- All personal data is stored and processed within the United Kingdom.
- We use a limited number of carefully vetted sub-processors, all subject to DPAs and annual security review.
- No personal data is transferred outside the UK without an appropriate safeguard (UK IDTA or equivalent).
- Full sub-processor list: [provisioniq.co.uk/sub-processors](https://provisioniq.co.uk/sub-processors)

## 6. Security Certifications

| Certification         | Details                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC 27001:2022    | ISMS certified. Annual surveillance audit.                                                                                                                    |
| Cyber Essentials Plus | Highest UK government cybersecurity standard. Renewed annually.                                                                                               |
| ICO Registration      | ProvisionIQ Ltd registered with the ICO under the Data Protection Act 2018. Registration No ZC156305.                                                         |
| Penetration Testing   | Annual external CREST-accredited penetration test. Critical/high findings remediated within 24/72 hours.                                                      |
| DPA 2018 Compliance   | Fully compliant with the UK Data Protection Act 2018 including the Law Enforcement Processing provisions and Schedule 1 conditions for special category data. |

## 7. Data Breach Obligations

- ProvisionIQ will notify affected Data Controllers within 48 hours of becoming aware of a personal data breach affecting their data.
- We maintain a Breach Register recording all incidents (including near-misses) for 3 years.
- Our Incident Response Policy ensures a structured response with clear ownership and communication timelines.
- We report to the ICO within 72 hours where we are the Data Controller for the affected data.

## 8. Contact

| Contact | Details |
|---------|---------|
|---------|---------|

|                                    |                            |
|------------------------------------|----------------------------|
| <b>Data Protection Officer</b>     | dpo@provisioniq.co.uk      |
| <b>General data enquiries</b>      | hello@provisioniq.co.uk    |
| <b>Security incidents</b>          | security@provisioniq.co.uk |
| <b>ICO (supervisory authority)</b> | ico.org.uk · 0303 123 1113 |

© ProvisionIQ Ltd 2026. Effective 22 May 2026. Registered in England & Wales, Co. No.17240497