Data Protection and Privacy (GDPR / UK GDPR Compliance)

April 2026

---

1. Purpose

The purpose of this policy is to ensure that Aqumen Business Solutions Limited ("the Company") complies with the requirements of the

The purpose of this policy is to ensure that Aqumen Business Solutions Limited ("the Company") complies with the requirements of the **UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and amendments introduced by the Data (Use and Access) Act 2025 (DUAA)**.

The Company is committed to protecting the privacy, confidentiality and security of personal data relating to employees, candidates, contractors, clients and other individuals whose data we process.

This policy applies to all staff, contractors and anyone else acting on behalf of the Company. Failure to comply may result in disciplinary action.

---

2. Scope

This policy applies to:

- Employees
- Temporary workers and contractors
- Job applicants and candidates
- Clients and business partners
- Any individual whose personal data is processed by the Company

It applies to all personal data processed by the Company in both **electronic and manual systems**.

---

3. Lawful Basis for Processing

The Company processes personal data only where there is a lawful basis under UK GDPR. These may include:

- Contractual necessity
- Legal obligation
- Legitimate interests
- Consent where required

Under the **Data (Use and Access) Act 2025**, the Company may also rely on **recognised legitimate interests**, which allow certain processing activities without a full balancing test where the processing relates to:

- Crime prevention or detection
- Safeguarding vulnerable individuals
- Responding to emergencies
- National security or public security purposes

The Company will ensure all processing activities remain fair, transparent and proportionate. The lawful basis for each processing activity is recorded in the Company's Records of Processing Activities (ROPA).

---

4. Categories of Personal Data

The Company may collect and process personal data including:

- Contact details
- Employment history and CV information
- Qualifications and professional memberships
- Right-to-work documentation
- Emergency contact details
- Payroll and tax information
- Performance and disciplinary information where applicable
- CCTV footage where used for security purposes

Additional information may be processed where necessary to fulfil legal or contractual obligations.

Special category data. Some personal data requires a higher level of protection — for example, information about health, disability, racial or ethnic origin, or religion. The Company does not routinely collect this type of data. Where it is necessary to do so, the Company will identify a lawful basis and a separate condition under Article 9 UK GDPR, obtain explicit consent where required, and apply additional security controls. Candidate CVs and application materials may contain special category data incidentally — staff must not submit such data to AI tools without prior management authorisation.

---

5. Use of Artificial Intelligence

The Company uses Matchmaker Software Limited, an AI-enabled recruitment platform, to support its day-to-day recruitment operations. The Kairos AI feature is a generative AI assistant — it does not make decisions about candidates and it does not score, rank or assess individuals. All decisions remain with the Company's staff.

The Kairos AI feature is used to assist staff with tasks including:

- Drafting job adverts and role descriptions
- Generating or reformatting candidate CVs
- Drafting candidate and client communications
- Summarising candidate information held in the platform

- Answering questions and providing general recruitment assistance in a conversational format

In using the AI feature, staff may input personal data relating to candidates or clients — for example, a candidate's name, work history or skills — in order to generate a draft document or response. That personal data is processed by OpenAI's API as part of generating the output.

Matchmaker Software Limited acts as a data processor on the Company's behalf. The Kairos AI feature is powered by **OpenAI's API. OpenAI (OpenAI OpCo, LLC, United States) acts as a sub-processor.** A written Data Processing Agreement is in place with Matchmaker Software Limited. Personal data transferred to OpenAI in the United States is protected by EU Standard Contractual Clauses with the UK Addendum.

The Company confirms that personal data submitted to the Kairos AI feature is not used to train, fine-tune or improve OpenAI's models. A Data Protection Impact Assessment (DPIA) is carried out before AI tools are deployed with live personal data.

Staff using the Kairos AI feature must:

- Only input personal data that is necessary for the task in hand
- Not input Special Category Data without prior management authorisation
- Review all AI-generated content before sending or using it — the AI assists, it does not decide
- Not rely on AI-generated output as a substitute for their own professional judgement

---

6. Data Subject Rights

Individuals whose data is processed by the Company have rights including:

- Right of access to personal data
- Right to correction of inaccurate data
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to object to processing
- Right to data portability

Subject Access Requests (DSARs) will normally be responded to within **30 days**.

In accordance with the **DUAA 2025 updates**:

- The Company is required to perform **reasonable and proportionate searches** when responding to DSARs rather than exhaustive searches.
- The response deadline may be paused where clarification of identity or request scope is required.

---

7. Right to Complain

Individuals have the right to raise concerns about how their personal data is handled.

From **19 June 2025**, individuals must first raise complaints directly with the Company before escalating to the Information Commissioner's Office (ICO). Raise complaints with **Andy Taylor, Aqumen Recruitment, Building 4, Carrwood Park, Selby Road, Leeds, LS15 4LG or by email to: andy.taylor@aqumenrecruitment.co.uk**

The Company will:

- Acknowledge complaints within **30 days**
- Investigate concerns without undue delay
- Provide a clear outcome and any corrective actions taken
- Maintain a written log of all complaints received and their outcomes

If an individual remains unsatisfied, they have the right to escalate to the ICO at www.ico.org.uk or by calling 0303 123 1113.

---

8. Data Sharing and International Transfers

Personal data may be shared with:

- Clients and prospective employers
- Payroll providers
- IT service providers
- AI-enabled recruitment software providers — specifically Matchmaker Software Limited (processor) and OpenAI (sub-processor)
- Professional advisers
- Regulatory bodies where required by law

Written Data Processing Agreements are in place with all third parties that process personal data on the Company's behalf. A register of all processor agreements is maintained and reviewed annually.

Where personal data is transferred internationally, the Company will ensure that the destination country provides a level of protection that is **not materially lower than the protections provided under UK data protection law**. Transfers to OpenAI in the United States are covered by EU Standard Contractual Clauses with the UK Addendum.

Risk-based assessments will be conducted before transfers occur.

---

9. Data Security

The Company implements appropriate organisational and technical measures to protect personal data from:

- Unauthorised access

- Loss or accidental destruction
- Unlawful processing
- Disclosure or misuse

All employees handling personal data must follow internal data security procedures and confidentiality obligations.

Personal data breach notification. Staff must report any suspected breach to management immediately. Where a breach is likely to result in a risk to individuals, the Company must notify the ICO within **72 hours** of becoming aware of it.

---

10. Data Retention

Personal data will only be retained for as long as necessary to fulfil the purpose for which it was collected, including legal, regulatory or contractual requirements. Indicative retention periods are:

- Unsuccessful candidate applications — 12 months from date of application. At the 12-month point the Company will contact the candidate to ask whether they wish to remain on the database. Where the candidate gives fresh consent, their data may be retained for a further period on that basis. Where no response is received or consent is declined, the data will be securely deleted.
- Successful placements and employee records — 6 years from end of engagement
- Payroll and tax records, including timesheets and working time data — 6 years from end of tax year (HMRC requirement and National Minimum Wage Act 1998)
- Right-to-work documentation — 2 years from end of engagement
- Client contact records — 6 years from end of relationship
- CCTV footage — 31 days unless required for an ongoing investigation

Where possible, data will be anonymised or securely deleted once it is no longer required.

---

11. Cookies and Online Tracking

The Company's websites may use cookies for functionality, security and analytics purposes.

Under updated UK privacy rules:

- Low-risk cookies for analytics or website functionality may be used without explicit consent where appropriate safeguards exist.
- Users must still be provided with **clear information and the ability to opt-out**.

Breaches of electronic communications regulations may result in significant financial penalties.

AQUMEN Recruitment

12. Responsibilities

All staff are responsible for:

- Protecting personal data they access or process
- Following Company data protection procedures
- Reporting suspected data breaches immediately

Management is responsible for ensuring that:

- Staff receive appropriate training
- Data protection controls are implemented
- Written Data Processing Agreements are in place with all processors
- DPIAs are completed before introducing new technologies that process personal data
- Compliance with UK data protection law is maintained

---

13. Policy Review

This policy will be reviewed at least annually to ensure compliance with evolving legislation and regulatory guidance, and immediately upon any material change to the law, to the Company's technology, or following a data breach.

Next scheduled review: April 2027.

ICO Registration Number: **Z3662926**

DocuSigned by:
Gill Taylor 09-Apr-26 | 14:04:23 BST
D78EC77F538B479...

April 2026

Gill Taylor
Managing Director