Data Processing Agreement

Complaix Ltd — Standard Data Processing Agreement Version 1.0 | Last reviewed: April 2026

---

1. Parties and Purpose

This Data Processing Agreement ("DPA") is entered into between **Complaix Ltd**, a company registered in England and Wales ("Processor"), and the organisation that has engaged Complaix Ltd under a Master Services Agreement, Order Form, or equivalent contract ("Controller").

This DPA forms part of, and is subject to, the terms of the agreement between the parties ("Principal Agreement"). In the event of any conflict between this DPA and the Principal Agreement, this DPA shall prevail in respect of data protection matters.

---

2. Definitions

The following terms have the meanings given to them in UK GDPR and EU GDPR as applicable:

- **"Personal Data"** means any information relating to an identified or identifiable natural person processed by Complaix Ltd on behalf of the Controller.
- **"Processing"** means any operation performed on Personal Data, including collection, storage, use, disclosure, and deletion.
- **"Data Subject"** means the natural person to whom Personal Data relates.
- **"Sub-Processor"** means any third party engaged by Complaix Ltd to process Personal Data on behalf of the Controller.

---

3. Subject Matter and Nature of Processing

Complaix Ltd processes Personal Data solely to provide the services described in the Principal Agreement, which may include:

- Hosting and operating the Complaix Platform on behalf of the Controller
- Generating AI Exposure Scores and governance artefacts from assessment data submitted by the Controller
- Providing Governance Advisory services, which may involve review of organisational data provided by the Controller
- Communicating with named contacts at the Controller's organisation

---

4. Categories of Personal Data and Data Subjects

Category	Examples	Data Subjects
Contact data	Name, email address, job title	Controller's employees and representatives
Assessment data	Organisational context, AI system descriptions, governance responses	Controller's employees completing assessments
Platform data	AI system registrations, decision log entries, governance artefacts	Controller's employees using the Platform
Usage data	Login events, feature usage (anonymised where possible)	Controller's employees using the Platform

---

5. Controller Obligations

The Controller warrants and represents that:

(a) It has a lawful basis for processing the Personal Data it provides to Complaix Ltd under applicable data protection law.

(b) It has provided all required notices to Data Subjects and obtained all necessary consents where required.

© It will promptly notify Complaix Ltd of any instruction that, in the Controller's reasonable opinion, may infringe applicable data protection law.

---

6. Processor Obligations

Complaix Ltd shall:

(a) Process Personal Data only on documented instructions from the Controller, unless required to do so by applicable law.

(b) Ensure that persons authorised to process Personal Data are subject to appropriate confidentiality obligations.

© Implement and maintain appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful processing, accidental loss, destruction, or damage, as set out in Annex A.

(d) Not engage Sub-Processors without prior written authorisation from the Controller, except as set out in Clause 9 below.

(e) Assist the Controller in responding to Data Subject requests, taking into account the nature of the processing.

(f) Assist the Controller in ensuring compliance with its obligations under Articles 32–36 of UK GDPR / EU GDPR, including security, breach notification, data protection impact assessments, and prior consultation.

(g) At the Controller's choice, delete or return all Personal Data to the Controller after the end of the provision of services, and delete existing copies unless applicable law requires storage.

(h) Make available to the Controller all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits and inspections.

---

7. Data Transfers

Complaix Ltd processes Personal Data within the United Kingdom and the European Economic Area by default. Where Personal Data is transferred outside the UK or EEA, Complaix Ltd shall ensure that appropriate safeguards are in place, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission or the UK ICO, as applicable
- Adequacy decisions where available
- Binding Corporate Rules where applicable

---

8. Security Measures

Complaix Ltd maintains the following technical and organisational security measures:

- Encryption of Personal Data in transit (TLS 1.2 minimum) and at rest (AES-256)
- Access controls based on the principle of least privilege
- Multi-factor authentication for all systems processing Personal Data
- Regular security assessments and penetration testing
- Incident response procedures with defined escalation paths
- Employee security awareness training

A full description of security measures is set out in Annex A.

---

9. Sub-Processors

The Controller provides general written authorisation for Complaix Ltd to engage the Sub-Processors listed in the Complaix Sub-Processor Register, available at **www.complaix.io/trust#sub-processors**.

Complaix Ltd shall:

(a) Notify the Controller at least 30 days in advance of any intended addition or replacement of Sub-Processors.

(b) Impose data protection obligations on Sub-Processors equivalent to those set out in this DPA.

© Remain fully liable to the Controller for the performance of Sub-Processors' obligations.

The Controller may object to a new Sub-Processor within 14 days of notification. Where the Controller objects and Complaix Ltd cannot accommodate the objection, the Controller may terminate the relevant services on written notice.

---

10. Data Subject Rights

Complaix Ltd shall, to the extent technically feasible, assist the Controller in fulfilling its obligations to respond to Data Subject requests. The Controller remains responsible for responding to Data Subjects directly. Complaix Ltd will notify the Controller without undue delay if it receives a Data Subject request relating to Personal Data processed on the Controller's behalf.

---

11. Personal Data Breaches

Complaix Ltd shall notify the Controller without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA. Notification shall include, to the extent available:

- The nature of the breach, including categories and approximate number of Data Subjects and records affected
- The name and contact details of the Data Protection contact at Complaix Ltd
- The likely consequences of the breach
- Measures taken or proposed to address the breach

---

12. Audit Rights

The Controller may, on reasonable written notice of no less than 30 days, conduct or commission an audit of Complaix Ltd's data processing activities covered by this DPA, no more than once per calendar year. Complaix Ltd may satisfy audit requests by providing up-to-date third-party audit reports (such as SOC 2 Type II reports) where these address the scope of the audit request.

---

13. Term and Termination

This DPA shall remain in force for the duration of the Principal Agreement. Upon termination or expiry of the Principal Agreement, Complaix Ltd shall, at the Controller's election, delete or return all Personal Data within 30 days, unless applicable law requires longer retention.

---

14. Governing Law

This DPA shall be governed by and construed in accordance with the laws of England and Wales. The parties submit to the exclusive jurisdiction of the courts of England and Wales.

---

15. Contact

Data Controller enquiries: privacy@complaix.io

Security disclosures: security@complaix.io

Complaix Ltd, United Kingdom

Annex A — Technical and Organisational Security Measures

Measure	Implementation
Encryption in transit	TLS 1.2 minimum on all external connections; TLS 1.3 preferred
Encryption at rest	AES-256 for all stored Personal Data
Access control	Role-based access control; principle of least privilege enforced
Authentication	Multi-factor authentication required for all staff accessing Personal Data
Network security	Firewall, DDoS protection via Cloudflare; private networking for database access
Vulnerability management	Regular automated scanning; annual penetration testing
Incident response	Documented IR plan; 72-hour breach notification commitment
Business continuity	Automated daily backups; tested recovery procedures
Employee training	Annual security awareness training; role-specific data protection training
Vendor management	Sub-Processor due diligence; DPAs with all Sub-Processors

---

This document is provided for informational purposes. For a countersigned DPA, contact compliance@complaix.io.