

# Data Processing Agreement

Part B · Article 28 UK GDPR · Addendum to the Subscription Agreement

This Data Processing Agreement forms part of the Principal Agreement between Vixio and the Controller. It is incorporated by reference into the Order Form and published at [vixio.com/trust](https://vixio.com/trust). In the event of conflict between this DPA and the Principal Agreement, this DPA prevails on data processing matters.

## Parties

|                 |                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Processor  | Compliance Online Limited t/a VIXIO Regulatory Intelligence (Co. No. 05706431), St Clare House, 33 Minories, London, EC3N 1DD ("Vixio" or "Processor") |
| Data Controller | The subscriber organisation named in the Order Form ("Controller")                                                                                     |
| Together        | The "Parties"                                                                                                                                          |
| Governing law   | England and Wales                                                                                                                                      |
| Published at    | <a href="https://vixio.com/trust">vixio.com/trust</a>                                                                                                  |

## Background

The Parties have entered into a Subscription Agreement (comprising an Order Form and Terms and Conditions) under which Vixio provides regulatory intelligence services (the "Principal Agreement"). In delivering those services, Vixio processes certain personal data on behalf of the Controller. This Data Processing Agreement ("DPA") sets out the terms on which Vixio does so and forms part of the Principal Agreement. In the event of conflict, this DPA prevails on data processing matters.

## B1. Definitions

|                             |                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Term                        | Definition                                                                                                                                |
| Data Protection Legislation | UK GDPR, the Data Protection Act 2018, and any successor or replacement legislation in force from time to time.                           |
| UK GDPR                     | The UK General Data Protection Regulation as defined in section 3(10) of the Data Protection Act 2018, as retained and amended in UK law. |

|                                       |                                                                                                                                                                                                       |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Controller</b>                     | The subscriber organisation named in the Order Form, which determines the purposes and means of processing Personal Data.                                                                             |
| <b>Processor</b>                      | Vixio, which processes Personal Data on behalf of the Controller.                                                                                                                                     |
| <b>Data Subject</b>                   | An identified or identifiable natural person whose Personal Data is processed under this DPA.                                                                                                         |
| <b>Personal Data</b>                  | Has the meaning given in Data Protection Legislation.                                                                                                                                                 |
| <b>Special Category Personal Data</b> | Has the meaning given in Article 9 UK GDPR, including data revealing racial or ethnic origin, health data, biometric data, and similar sensitive categories.                                          |
| <b>Personal Data Breach</b>           | Has the meaning given in Data Protection Legislation — a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. |
| <b>Services</b>                       | The subscription services provided by Vixio under the Principal Agreement, including the Vixio platform, VIQ, SCANS, Workspace, and related features.                                                 |
| <b>Sub-processor</b>                  | Any third party engaged by Vixio to process Personal Data on Vixio's behalf in connection with the Services.                                                                                          |
| <b>AI Features</b>                    | VIQ, SCANS, the Workspace Document Library AI functions, and related AI-enabled workflows forming part of the Services.                                                                               |
| <b>Customer Inputs</b>                | Prompts, queries, document content, and other data submitted by the Controller or its authorised users through the AI Features.                                                                       |
| <b>Workspace Document Library</b>     | The persistent document storage feature within Workspace enabling subscribers to upload, store, and use documents in connection with the Services, including AI Features.                             |
| <b>Principal Agreement</b>            | The Order Form and Terms and Conditions entered into between the Parties, to which this DPA is an addendum.                                                                                           |

## B2. Scope and Nature of Processing

### B2.1 Role of the Parties

The Controller determines the purposes and means of processing Personal Data in connection with the Services. Vixio processes Personal Data solely as a data processor, acting on the Controller's documented instructions as set out in this DPA and the Principal Agreement.

### B2.2 Processing Parameters

|                       |                                                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject matter</b> | Processing of Personal Data of the Controller's authorised users and any other individuals whose data is submitted to the Services by or on behalf of the Controller                                                  |
| <b>Duration</b>       | Term of the Principal Agreement, plus the deletion and return period following termination as set out in Clause B3.9                                                                                                  |
| <b>Nature</b>         | Storage, access management, usage logging, AI Feature processing, document ingestion and retrieval, communications, analytics                                                                                         |
| <b>Purpose</b>        | Service delivery; user authentication and access control; security monitoring and fraud prevention; support and incident management; legal compliance; service improvement on an aggregated and anonymised basis only |
| <b>Data types</b>     | See Schedule B1                                                                                                                                                                                                       |
| <b>Data subjects</b>  | See Schedule B1                                                                                                                                                                                                       |

## B2.3 Instructions

Vixio shall process Personal Data only on the Controller's documented instructions. The Principal Agreement and this DPA constitute the Controller's instructions as at the date of execution. If required by applicable law to process Personal Data otherwise than on the Controller's instructions, Vixio shall inform the Controller of that requirement before processing, unless legally prohibited from doing so. If Vixio considers that any instruction from the Controller infringes Data Protection Legislation, it shall promptly notify the Controller.

## B3. Vixio's Obligations

### B3.1 Confidentiality

Vixio shall ensure that all persons authorised to process Personal Data under this DPA are subject to binding obligations of confidentiality in respect of that data, whether by contract or by operation of law. Such obligations shall survive the termination or expiry of this DPA.

### B3.2 Security

Vixio shall implement and maintain appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access, having regard to the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The minimum measures maintained by Vixio are set out in Schedule B2.

### B3.3 Sub-processors

**B3.3.1** Vixio shall provide the Controller with not less than thirty (30) days' prior written notice before engaging any net-new Sub-processor not previously listed in Part C of this document set.

**B3.3.2** The Controller may object to the addition of a net-new Sub-processor by written notice within fourteen (14) days of receiving Vixio's notification. Where the Controller raises a reasonable objection that cannot be resolved within a further fourteen (14) days, the Controller may terminate the affected Services on written notice, without penalty in respect of the termination.

**B3.3.3** Sub-processors are engaged under written contracts imposing data protection, confidentiality, and security obligations no less protective than those in this DPA.

**B3.3.4** Vixio remains fully liable to the Controller for the acts and omissions of its Sub-processors to the same extent as it would be liable for its own acts and omissions.

**B3.3.5** General authorisation is given by the Controller for the Sub-processors listed in Part C as at the date of this DPA. Model version changes, upgrades, or substitutions within an existing approved Sub-processor relationship do not constitute the engagement of a new Sub-processor and do not trigger the notice obligation in B3.3.1.

## **B3.4 Data Subject Rights**

Vixio shall, taking into account the nature of processing, provide reasonable assistance to the Controller to fulfil its obligations under Data Protection Legislation to respond to requests from Data Subjects exercising their rights. Where Vixio receives a data subject rights request directly from a Data Subject in relation to Personal Data processed under this DPA, Vixio shall forward that request to the Controller within five (5) business days and shall not respond directly to the Data Subject without the Controller's prior written authorisation.

## **B3.5 Compliance Assistance**

Vixio shall provide reasonable assistance to the Controller in connection with: (a) compliance with the Controller's security obligations under Article 32 UK GDPR; (b) notification of Personal Data Breaches to supervisory authorities and Data Subjects under Articles 33 and 34 UK GDPR; (c) data protection impact assessments under Article 35 UK GDPR; and (d) prior consultation with supervisory authorities under Article 36 UK GDPR. Assistance beyond one data protection impact assessment per calendar year may be subject to Vixio's reasonable time and costs.

## **B3.6 Breach Notification**

Vixio shall notify the Controller without undue delay, and in any event within forty-eight (48) hours of becoming aware, of a confirmed or reasonably suspected Personal Data Breach affecting Personal Data processed under this DPA. Such notification shall include, to the extent then known: (a) the nature of the Breach, including the categories and approximate number of Data Subjects and Personal Data records affected; (b) the name and contact details of Vixio's data protection contact; (c) the likely consequences of the Breach; and (d) the measures taken or proposed to address the Breach and mitigate its effects. Where all required information is not available at the time of initial notification, Vixio shall provide it in phases as it becomes available.

## **B3.7 Records of Processing**

Vixio shall maintain records of processing activities carried out on behalf of the Controller as required by Article 30(2) UK GDPR and shall make such records available to the Controller or a competent supervisory authority on request.

### **B3.8 Audit Rights**

On not less than thirty (30) days' prior written notice, Vixio shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and shall permit and contribute to audits and inspections conducted by the Controller or a third-party auditor appointed by the Controller. Audit rights are limited to once per calendar year, except where a confirmed Personal Data Breach has occurred. Vixio may satisfy its audit obligations by providing up-to-date ISO 27001 certificates, SOC 2 reports (when available), or the results of a mutually agreed third-party audit. Any on-site audit shall be conducted at the Controller's cost and at times agreed with Vixio to minimise disruption to its business. Audit results constitute Vixio's confidential information and the Controller shall implement appropriate measures to protect their confidentiality.

### **B3.9 Return and Deletion of Data**

Within thirty (30) days of termination of the Principal Agreement or receipt of a written request from the Controller, Vixio shall at the Controller's election either: (a) return all Personal Data to the Controller in a commonly used, machine-readable format; or (b) securely delete all Personal Data and provide written confirmation of deletion. Vixio may retain Personal Data beyond this period only to the extent required by applicable law, and shall notify the Controller of any such retention obligation. Documents stored in the Workspace Document Library are deleted in accordance with this clause. Aggregated and anonymised Usage Data from which no individual can be identified may be retained by Vixio indefinitely.

## **B4. Controller's Obligations**

The Controller represents, warrants, and undertakes that:

- It has a valid lawful basis under Data Protection Legislation for providing Personal Data to Vixio and instructing Vixio to process it in connection with the Services.
- All required notices have been given to, and all required consents obtained from, Data Subjects whose Personal Data is submitted to the Services.
- The Controller is solely responsible for the accuracy, quality, and legality of Personal Data submitted to the Services.
- The Controller's instructions to Vixio comply with Data Protection Legislation.
- The Controller shall not submit Special Category Personal Data to the AI Features or Workspace Document Library unless a specific written arrangement addressing the additional safeguards required for such data has been agreed in advance with Vixio.
- The Controller shall ensure that all authorised users comply with the Terms and Conditions and this DPA when accessing the Services.

## **B5. AI Features and Data Use**

### **B5.1 Model Training Commitment**

Vixio confirms that: (a) Personal Data and Customer Inputs processed through the AI Features are not used to train foundation models for the benefit of other customers; and (b) AI Sub-processors are contractually restricted from using Customer data submitted through the Services to train or

improve foundation models, except where explicitly authorised by Vixio and appropriately configured within the relevant managed platform environment.

## **B5.2 Workspace Document Library**

Documents uploaded to the Workspace Document Library are stored within Vixio's cloud infrastructure (Amazon Web Services) under the terms of this DPA. When a document is used in connection with an AI Feature, the document content is processed transiently through the AI pipeline. Source documents are not persistently stored within AI sub-processor infrastructure. On termination, documents are deleted in accordance with Clause B3.9.

## **B5.3 Model Selection**

Foundation models deployed in connection with the Services may change as part of Vixio's continuous model evaluation and optimisation programme. Model changes within an approved Sub-processor relationship do not trigger the Sub-processor notice obligations in Clause B3.3.1. The current models in use are listed in Part C of this document set, which is updated at [vixio.com/trust](https://vixio.com/trust).

## **B5.4 AI Output Disclaimer**

Outputs generated by AI Features are for information and research purposes only. They do not constitute legal, regulatory, compliance, or expert advice. The Controller is responsible for verifying the accuracy and applicability of AI outputs before relying on them. Vixio's liability for AI outputs is governed by the liability provisions of the Principal Agreement.

# **B6. International Data Transfers**

## **B6.1 Transfer Mechanisms**

Where Personal Data processed under this DPA is transferred outside the United Kingdom, Vixio relies on one or more of the following safeguards: (a) Standard Contractual Clauses approved by the European Commission, together with the UK Addendum issued by the ICO pursuant to section 119A of the Data Protection Act 2018; (b) UK International Data Transfer Agreements issued by the ICO; or (c) adequacy regulations made under section 17A of the Data Protection Act 2018. The applicable mechanism for each Sub-processor is set out in Part C.

## **B6.2 Controller Authorisation**

The Controller authorises Vixio to enter into the relevant transfer mechanisms with Sub-processors on the Controller's behalf where required to give effect to the lawful transfer of Personal Data. Copies of applicable transfer mechanisms are available on written request to [dataprotection@vixio.com](mailto:dataprotection@vixio.com).

# **B7. Liability**

Each Party's liability under this DPA is subject to the limitations and exclusions set out in the Principal Agreement, save that nothing in this DPA or the Principal Agreement limits or excludes liability for: (a) death or personal injury caused by negligence; (b) fraud or fraudulent



misrepresentation; or (c) any liability that cannot lawfully be limited or excluded under applicable law, including Data Protection Legislation.

For the avoidance of doubt, Vixio's liability for breaches of this DPA is subject to the aggregate liability cap set out in the Principal Agreement, unless otherwise agreed in writing.

## **B8. Term and Termination**

This DPA comes into effect on the date of the Order Form and continues for the duration of the Principal Agreement. Termination or expiry of the Principal Agreement automatically terminates this DPA, subject to Clause B3.9 (Return and Deletion) and the survival provisions below. The following clauses survive termination or expiry of this DPA: B3.1 (Confidentiality), B3.4 (Data Subject Rights), B3.7 (Records), B3.8 (Audit Rights), B3.9 (Return and Deletion), B7 (Liability), and B9 (General).

## **B9. General**

### **B9.1 Governing Law**

This DPA is governed by the laws of England and Wales. The Parties submit to the exclusive jurisdiction of the courts of England and Wales in respect of any dispute arising under or in connection with this DPA.

### **B9.2 Entire Agreement**

This DPA, together with the Principal Agreement and the documents incorporated by reference (including Part C — AI Sub-processors Schedule and the Privacy Policy), constitutes the entire agreement between the Parties in respect of the processing of Personal Data under the Services.

### **B9.3 Amendments**

Vixio may update this DPA by providing not less than thirty (30) days' prior written notice of material changes. The current version of this DPA is published at [vixio.com/trust](https://vixio.com/trust) and the version incorporated into any Order Form is the version current at the date of that Order Form unless otherwise agreed in writing.

### **B9.4 Priority**

In the event of conflict or inconsistency between this DPA and the Principal Agreement, this DPA takes precedence on data processing matters only.

### **B9.5 Severability**

If any provision of this DPA is held to be invalid, illegal, or unenforceable in any respect, such provision shall be modified to the minimum extent necessary to make it enforceable, and the validity and enforceability of the remaining provisions shall not be affected.

## **Execution**

**This DPA is entered into as an addendum to the Order Form. Execution of the Order Form by both parties constitutes acceptance of this DPA. Where separate execution is required, both parties must sign below.**

**FOR AND ON BEHALF OF VIXIO (DATA PROCESSOR)**

Legal entity: Compliance Online Limited t/a VIXIO Regulatory Intelligence

Address: St Clare House, 33 Minories, London, EC3N 1DD

Signed by: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**FOR AND ON BEHALF OF THE CONTROLLER**

Legal entity: [Controller legal entity — as per Order Form]

Address: [Controller registered address — as per Order Form]

Signed by: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## Schedule B1 — Processing Description

### 1. Subject Matter

Processing of Personal Data of the Controller's authorised users and any other individuals whose personal data is submitted to the Services by or on behalf of the Controller, in connection with Vixio's provision of the Services.

### 2. Duration

The term of the Principal Agreement. Post-termination: the period required to fulfil deletion and return obligations under Clause B3.9.

### 3. Nature of Processing

| Activity | Description                                                                                        |
|----------|----------------------------------------------------------------------------------------------------|
| Storage  | Personal Data stored within Vixio's cloud infrastructure (AWS) for the purpose of service delivery |



|                                         |                                                                                                                                                                                       |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access management</b>                | User authentication, session management, and licence enforcement                                                                                                                      |
| <b>Usage logging</b>                    | Recording of user activity for security monitoring, audit, and usage analytics                                                                                                        |
| <b>AI Feature processing</b>            | Customer Inputs (prompts and document content) and associated metadata transmitted to AI Sub-processors where AI Features are used                                                    |
| <b>Document ingestion and retrieval</b> | Documents uploaded to the Workspace Document Library stored in Vixio's AWS infrastructure; document content called transiently into AI processing pipelines when AI Features are used |
| <b>Communications</b>                   | Platform notifications, service updates, and support communications                                                                                                                   |
| <b>Analytics</b>                        | Aggregated and anonymised analysis of usage patterns for service improvement                                                                                                          |

## 4. Purpose

- Service delivery and platform operation
- User authentication and access control
- Security monitoring and fraud prevention
- Support and incident management
- Legal and regulatory compliance
- Service improvement on an aggregated and anonymised basis only

## 5. Types of Personal Data

| Category                | Examples                                                                                                                                                            |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identity</b>         | First name, last name, job title                                                                                                                                    |
| <b>Contact</b>          | Work email address, telephone number                                                                                                                                |
| <b>Technical</b>        | IP address, device type, browser type and version, session identifiers, login timestamps                                                                            |
| <b>Usage</b>            | Pages visited, search queries, VIQ prompts and queries, feature interactions                                                                                        |
| <b>Document content</b> | Content of documents uploaded to the Workspace Document Library by the Controller or its authorised users — may include Personal Data depending on document content |
| <b>Communications</b>   | Support ticket content, email correspondence with Vixio's support and account management teams                                                                      |

**Note on Special Category Personal Data:** The Controller should not submit Special Category Personal Data to the Services unless a specific written arrangement has been agreed with Vixio in advance. See Clause B4.

**Note on VIQ prompt retention:** VIQ prompts submitted by authorised users are logged as usage data. Where prompts contain information that identifies or could identify a natural person, they constitute Personal Data. Prompts are retained for [INSERT RETENTION PERIOD — confirm with engineering] and then deleted, unless retention is required by law.

6. Categories of Data Subjects

- Employees and contractors of the Controller who are authorised users of the Services
- Any other individuals whose Personal Data is submitted to the Services by or on behalf of the Controller, including through the Workspace Document Library

Schedule B2 — Technical and Organisational Security Measures

This Schedule sets out the minimum technical and organisational security measures maintained by Vixio in fulfilment of its obligations under Article 28(3)(c) and Article 32 UK GDPR. These measures are consistent with Vixio's ISO/IEC 27001:2022 certified Information Security Management System (Certificate No. 267181, valid to 05 October 2028, issued by British Assessment Bureau, UKAS accreditation 8289).

Organisational Measures

| Measure                     | Description                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Information Security Policy | Documented policy aligned to ISO/IEC 27001:2022, reviewed annually or following material changes to the organisation, systems, or threat landscape                                                             |
| ISO 27001 ISMS              | Information Security Management System certified to ISO/IEC 27001:2022 (Certificate No. 267181, valid to 05 October 2028). Subject to annual surveillance assessments by British Assessment Bureau (UKAS 8289) |
| Cyber Essentials            | Certified under the UK Government's Cyber Essentials scheme                                                                                                                                                    |
| Security roles              | Designated security responsibilities within the technology team; CTO acts as ISMS Lead                                                                                                                         |
| Employee training           | Security awareness training provided on onboarding and annually thereafter                                                                                                                                     |
| Confidentiality obligations | All staff and contractors subject to binding confidentiality obligations as a condition of engagement                                                                                                          |

|                                    |                                                                                                                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Third-party risk management</b> | Sub-processors assessed against security, data protection, and business continuity criteria prior to onboarding and periodically thereafter; subject to written data processing terms |
| <b>Vulnerability disclosure</b>    | Responsible disclosure programme — report to tech@vixio.com (PGP encrypted)                                                                                                           |
| <b>Incident response</b>           | Documented incident response procedure; breach notification to Controller within 48 hours of confirmed or suspected breach                                                            |

## Technical Measures

| Measure                             | Description                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Encryption in transit</b>        | TLS 1.2 or higher enforced across all platform communications                                                                                                                                                                                                                                 |
| <b>Encryption at rest</b>           | All cloud-hosted Personal Data encrypted at rest                                                                                                                                                                                                                                              |
| <b>Access controls</b>              | Role-based access control (RBAC); principle of least privilege enforced across all environments                                                                                                                                                                                               |
| <b>Authentication</b>               | Multi-factor authentication (MFA) enforced for all Vixio staff on production systems; SSO available for enterprise subscribers                                                                                                                                                                |
| <b>Privileged access management</b> | Privileged access to infrastructure subject to additional controls and quarterly access reviews                                                                                                                                                                                               |
| <b>Logging and monitoring</b>       | Centralised access logging; security event monitoring with automated alerting                                                                                                                                                                                                                 |
| <b>Vulnerability management</b>     | Regular vulnerability scanning; annual penetration testing by qualified third-party provider                                                                                                                                                                                                  |
| <b>Backup and recovery</b>          | Regular automated backups; documented disaster recovery procedures; recovery objectives reviewed annually                                                                                                                                                                                     |
| <b>Network security</b>             | Network segmentation; firewall controls; intrusion detection                                                                                                                                                                                                                                  |
| <b>AI security boundary</b>         | AI features accessed via enterprise-managed platforms (AWS Bedrock, Azure OpenAI Service, Google Vertex AI) providing controlled execution environments, data isolation, and enterprise-grade security controls. Customer data does not leave Vixio's account boundary within these platforms |
| <b>Document library security</b>    | Workspace Document Library content stored within Vixio's AWS infrastructure; access controlled by subscriber authentication; content isolated per subscriber account                                                                                                                          |

