

Fisar

DATA PRIVACY POLICY

Last Updated: August 2026

1. INTRODUCTION

Fisar UK Ltd ("Fisar", "we", "us", or "our") is committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, store, and protect personal data when you:

- Visit our website (www.fisar.co.uk);
- Use our Fisar software-as-a-service platform (the "Platform" or "Services");
- Contact us via our contact form, email, telephone, or other means;
- Interact with us as a customer, prospective customer, or business contact; or
- Are a data subject whose personal data is processed through our Platform on behalf of our customers.

This Privacy Policy should be read alongside our Terms & Conditions, which govern use of our Services.

About Fisar

Fisar provides an automated Subject Access Request (SAR) processing platform that helps organisations respond efficiently and compliantly to data subject requests under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Data Controller Information

Fisar UK Ltd is the data controller for personal data collected through our website, contact forms, and in connection with our business relationships. For personal data processed through our Platform on behalf of customers, our customers are the data controllers and Fisar acts as a data processor.

Company Details

- **Company Name:** Fisar UK Ltd
- **Company Number:** 16926890
- **Registered Address:** Second Floor, Sutherland House, 70-78 West Hendon Broadway, London, United Kingdom, NW9 7BT
- **Email:** info@fisar.co.uk
- **Telephone:** 02046420600

2. PERSONAL DATA WE COLLECT

We collect different types of personal data depending on how you interact with us:

2.1 Website Visitors

When you visit our website, we may automatically collect:

- **Technical data:** IP address, browser type and version, operating system, device type, screen resolution;
- **Usage data:** pages visited, time spent on pages, navigation paths, referring website;
- **Cookie data:** as described in our Cookie section below.

2.2 Contact Form Submissions

When you submit an enquiry through our contact form, we collect:

- Name;
- Email address;
- Telephone number (if provided);
- Organisation name (if provided);
- Your message or enquiry;
- Date and time of submission.

2.3 Email Correspondence

When you correspond with us by email, we collect and retain:

- Your email address;
- Name and any other personal data included in the email;
- The content of the correspondence;
- Attachments (if any);
- Date and time of correspondence.

2.4 Platform Users (Customers and Authorised Users)

When you register for or use our Platform, we collect:

- **Account information:** name, email address, job title, organisation name;
- **Authentication data:** username, encrypted password, multi-factor authentication details;
- **Billing information:** billing contact details, payment information (processed by our payment provider);
- **Usage data:** login history, features used, actions performed within the Platform;
- **Support data:** support tickets, communications with our support team.

2.5 Data Processed on Behalf of Customers (SAR Data)

Our Platform processes personal data on behalf of our customers in connection with Subject Access Requests. This may include any category of personal data that our customers' data subjects have requested, such as:

- Identity information (names, dates of birth, identification numbers);
- Contact information (addresses, email addresses, telephone numbers);
- Employment information;
- Educational records;

- Health information;
- Financial information;
- Any other personal data held by the organisation about the data subject.

Important: For SAR Data, our customers are the data controllers. Fisar processes this data solely on our customers' instructions as a data processor. Please refer to Section 6 for details on how SAR Data is handled.

3. HOW WE USE YOUR PERSONAL DATA

We use personal data for the following purposes:

3.1 Website Operation and Improvement

- To operate, maintain, and improve our website;
- To analyse website usage and optimise user experience;
- To ensure website security and prevent fraud.

Legal basis: Legitimate interests (operating and improving our website).

3.2 Responding to Enquiries

- To respond to enquiries submitted via our contact form;
- To provide information about our Services;
- To follow up on your enquiry where appropriate.

Legal basis: Legitimate interests (responding to enquiries); or consent (where you have specifically requested information).

3.3 Email Communications

- To respond to your correspondence;
- To maintain records of our communications;
- To provide customer support.

Legal basis: Legitimate interests (managing business communications); contract performance (where related to our Services).

3.4 Providing Our Services

- To create and manage your account;
- To provide access to the Platform;
- To process and fulfil your subscription;
- To provide customer support;
- To send service-related communications (e.g., updates, security alerts, maintenance notices).

Legal basis: Contract performance (providing Services you have subscribed to).

3.5 Billing and Payments

- To process payments for our Services;
- To send invoices and payment reminders;

- To manage billing queries.

Legal basis: Contract performance; legal obligation (maintaining financial records).

3.6 Marketing (with consent)

- To send marketing communications about our Services (only where you have consented);
- To invite you to events, webinars, or provide industry updates.

Legal basis: Consent. You may withdraw consent at any time by clicking 'unsubscribe' in any marketing email or contacting us.

3.7 Legal and Compliance

- To comply with legal obligations;
- To establish, exercise, or defend legal claims;
- To respond to lawful requests from public authorities.

Legal basis: Legal obligation; legitimate interests (protecting our legal rights).

4. DATA RETENTION

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Our specific retention periods are:

Data Category	Retention Period	Reason
Website analytics data	26 months	Industry standard for analytics; anonymised after this period
Contact form submissions	2 years from submission, or duration of any resulting business relationship plus 2 years	To respond to and follow up on enquiries; to maintain records of how relationships began
Email correspondence	Duration of business relationship plus 6 years	Contractual and legal record-keeping; limitation period for contract claims
Customer account data	Duration of subscription plus 6 years	Contract performance; legal and regulatory requirements; limitation periods
Billing and payment records	7 years from transaction	Legal requirement (tax and accounting records)
Platform usage logs	12 months	Security monitoring; service improvement; support
Marketing preferences	Until consent withdrawn, then 12 months suppression	To honour opt-out requests
SAR Data (client data processed through Platform)	Only until secure delivery to data subject, then immediately purged	See Section 6 for full details

At the end of the applicable retention period, personal data will be securely deleted or anonymised.

5. COOKIES AND SIMILAR TECHNOLOGIES

Our website uses cookies and similar technologies to enhance your browsing experience and analyse website usage.

5.1 What Are Cookies?

Cookies are small text files placed on your device when you visit a website. They help the website recognise your device and remember certain information about your visit.

5.2 Types of Cookies We Use

Strictly Necessary Cookies

These cookies are essential for the website to function and cannot be switched off. They are usually set in response to actions you take, such as setting privacy preferences or logging in.

Performance/Analytics Cookies

These cookies help us understand how visitors interact with our website by collecting information anonymously. We use this data to improve our website.

Functional Cookies

These cookies enable enhanced functionality and personalisation, such as remembering your preferences.

5.3 Managing Cookies

When you first visit our website, you will be presented with a cookie banner allowing you to accept or reject non-essential cookies. You can change your preferences at any time through our cookie settings or by adjusting your browser settings.

Please note that blocking certain cookies may affect your experience of our website.

5.4 Third-Party Cookies

Some cookies are placed by third-party services that appear on our pages. We do not control these cookies. Please refer to the relevant third party's privacy policy for more information.

6. PROCESSING OF SUBJECT ACCESS REQUEST DATA

This section specifically addresses how personal data is processed through our Platform in connection with Subject Access Requests.

6.1 Fisar's Role

When our customers use the Fisar Platform to process Subject Access Requests, Fisar acts as a data processor. Our customers (the organisations responding to SARs) remain the data controllers and are responsible for ensuring their processing is lawful.

If you are a data subject whose data is being processed through our Platform, please contact the organisation from which you made your Subject Access Request for information about how your data is being handled.

6.2 How SAR Data is Processed

The Fisar Platform:

- Verifies the identity of data subjects making requests;
- Retrieves personal data from our customers' systems through secure integrations;
- Searches for and identifies Personal Identifiable Information (PII) within documents;
- Removes duplicate documents to streamline the response;
- Provides tools for redaction of third-party data, exempt information, and sensitive content within text, images, audio, and video;
- Enables secure, encrypted delivery of the SAR response to the data subject.

6.3 Preview and Manual Redaction

Fisar provides a Preview Mode that allows authorised users, including Data Protection Officers (DPOs), to review files before completing a Subject Access Request. In Preview Mode, a DPO can open and view an individual file in an editor and manually redact any personal data, third-party information, exempt information, or other content that may not have been identified automatically.

Preview Mode can be used in two ways:

- **Single File Preview:** The DPO can upload a single file directly into Preview Mode for review and manual redaction.
- **Processed SAR Preview:** The DPO can attach a previously processed SAR to Preview Mode and review its files individually, making any additional manual redactions required before the SAR is finalised.

Files uploaded directly for Preview Mode, as well as files associated with a processed SAR, are subject to Fisar's standard data retention period of **30 days**, after which they are securely deleted in accordance with Fisar's data retention and deletion procedures.

Only authorised users with the appropriate access permissions can access and manually redact files through Preview Mode. Manual redactions performed within the Platform are recorded as part of Fisar's audit trail.

6.4 Data Retention for SAR Data

SAR Data is retained only for as long as is necessary to securely deliver the information to the data subject.

Our data handling process is as follows:

- SAR Data is processed within our secure Platform;
- Once the data subject downloads their SAR response, the data is immediately and permanently purged from our systems;
- After purging, the only copies of the SAR response will remain with:
 - The data subject (who received their data); and
 - The organisation that responded to the SAR (our customer), in accordance with their own retention policies.

Fisar does not retain any copies of SAR Data after secure delivery and purging. This approach ensures data minimisation and protects the privacy of data subjects.

6.5 Security of SAR Data

Given the sensitive nature of SAR Data, we implement stringent security measures including:

- Encryption in transit (TLS 1.2 or higher) and at rest (AES-256);
- Secure, authenticated access controls;
- Audit logging of all data access;
- Regular security assessments and penetration testing;
- Secure deletion processes that render data unrecoverable.

6.6 Sub-processors

We may use sub-processors to assist in providing our Services. A current list of sub-processors is available on request. All sub-processors are bound by data processing agreements that provide equivalent protection to that set out in our customer contracts.

7. WHO WE SHARE YOUR DATA WITH

We may share your personal data with the following categories of recipients:

7.1 Service Providers

We use trusted third-party service providers who process data on our behalf, including:

- Cloud hosting providers (for Platform infrastructure);
- Payment processors (for billing);
- Email service providers (for communications);
- Analytics providers (for website analytics);
- Customer support tools.

All service providers are contractually bound to protect your data and use it only for the purposes we specify.

7.2 Professional Advisers

We may share data with our professional advisers (lawyers, accountants, auditors) where necessary for legal, accounting, or audit purposes.

7.3 Legal and Regulatory

We may disclose personal data where required by law, regulation, legal process, or governmental request, or where necessary to protect our rights, property, or safety, or that of others.

7.4 Business Transfers

If Fisar is involved in a merger, acquisition, or sale of assets, your personal data may be transferred as part of that transaction. We will notify you of any such change and any choices you may have.

7.5 With Your Consent

We may share your data with other parties where you have given us specific consent to do so.

We do not sell your personal data to third parties.

8. INTERNATIONAL DATA TRANSFERS

Fisar is based in the United Kingdom. Where possible, we process and store personal data within the UK and European Economic Area (EEA).

Where we transfer personal data outside the UK/EEA, we ensure appropriate safeguards are in place, including:

- Transfers to countries with an adequacy decision from the UK Government or European Commission;
- Use of Standard Contractual Clauses (SCCs) approved by the UK Information Commissioner;
- Other appropriate safeguards as permitted under UK GDPR.

You may request a copy of the safeguards we use by contacting us.

9. DATA SECURITY

We take the security of your personal data seriously and implement appropriate technical and organisational measures to protect it against unauthorised access, loss, destruction, or alteration.

Our security measures include:

- Encryption of data in transit and at rest;
- Secure access controls and authentication;
- Regular security assessments and penetration testing;
- Employee training on data protection and security;
- Incident response procedures;
- Regular backups stored securely;
- Physical security of our facilities and those of our hosting providers.

We maintain security certifications and compliance with industry standards. Details are available on request.

While we implement robust security measures, no method of transmission over the internet or electronic storage is 100% secure. We cannot guarantee absolute security but are committed to protecting your data to the highest practicable standard.

10. YOUR DATA PROTECTION RIGHTS

Under UK data protection law, you have the following rights regarding your personal data:

10.1 Right of Access

You have the right to request a copy of the personal data we hold about you and information about how we process it.

10.2 Right to Rectification

You have the right to request correction of inaccurate personal data and completion of incomplete data.

10.3 Right to Erasure

You have the right to request deletion of your personal data in certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected.

10.4 Right to Restrict Processing

You have the right to request restriction of processing in certain circumstances, such as when you contest the accuracy of the data.

10.5 Right to Data Portability

You have the right to receive your personal data in a structured, commonly used, machine-readable format and to transmit it to another controller, where technically feasible.

10.6 Right to Object

You have the right to object to processing based on legitimate interests or for direct marketing purposes.

10.7 Rights Related to Automated Decision-Making

You have rights in relation to automated decision-making and profiling. We do not currently make decisions based solely on automated processing that produce legal or similarly significant effects.

10.8 Right to Withdraw Consent

Where we process your data based on consent, you have the right to withdraw that consent at any time. This will not affect the lawfulness of processing before withdrawal.

Exercising Your Rights

To exercise any of these rights, please contact us using the details in Section 13. We will respond to your request within one month. This period may be extended by a further two months for complex requests, in which case we will inform you.

We may need to verify your identity before processing your request. There is generally no fee for exercising your rights, but we may charge a reasonable fee or refuse to act on a request if it is manifestly unfounded or excessive.

Complaints

If you are not satisfied with how we handle your request or have concerns about our data processing, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

- **Website:** www.ico.org.uk
- **Telephone:** 0303 123 1113
- **Address:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

11. CHILDREN'S DATA

Our website and Services are not directed at children under 18 years of age, and we do not knowingly collect personal data from children through our website or direct interactions.

Where our customers process SAR Data through our Platform that relates to children, this is done under our customers' controllership and in accordance with their legal obligations.

If we become aware that we have inadvertently collected personal data from a child without appropriate consent, we will take steps to delete that information as soon as possible.

12. THIRD-PARTY LINKS

Our website may contain links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you.

We do not control these third-party websites and are not responsible for their privacy practices or content. We encourage you to read the privacy policy of every website you visit.

13. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or for other operational reasons.

When we make changes:

- We will update the "Last Updated" date at the top of this policy;
- For material changes, we will provide prominent notice on our website or notify you directly where appropriate;
- We encourage you to review this policy periodically.

Continued use of our website or Services after changes are posted constitutes acceptance of the revised policy.

14. CONTACT US

If you have any questions about this Privacy Policy, wish to exercise your data protection rights, or have any concerns about how we handle your personal data, please contact us:

Fisar UK Ltd

Second Floor, Sutherland House
70-78 West Hendon Broadway
London, United Kingdom
NW9 7BT

Email: info@fisar.co.uk

Telephone: 02046420600

We aim to respond to all enquiries within 5 business days.

Fisar UK Ltd

- **Company Number:** 16926890
- **Registered Address:** Second Floor, Sutherland House, 70-78 West Hendon Broadway, London, NW9 7BT
- **Email:** info@fisar.co.uk
- **Telephone:** 02046420600