
fitzrovia

LAST UPDATE DATE 22/6/2026

PRIVACY POLICY

IMPORTANT NOTICE

This Privacy Policy applies to all personal data collected, processed, and stored by Fitzrovia IT Limited ("we", "us", or "our"). It is compliant with the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR 2016/679), the Data Protection Act 2018, and other applicable data protection legislation. Please read this policy carefully.

1. About This Privacy Policy

This Privacy Policy explains how Fitzrovia IT Limited (registered in England under company number 03720812, whose registered office is at 1st Floor Arthur Stanley House, 40-50 Tottenham Street, London, United Kingdom, W1T 4RN) collects, uses, shares, stores, and protects your personal data.

This policy applies to:

- All visitors to our website at www.fitzroviait.com
- Customers, prospective customers, and subscribers

- Business contacts, partners, and suppliers
- Job applicants and contractors
- Any individual whose personal data we process in the course of our business activities

We are committed to protecting your privacy and handling your personal data in an open, transparent, and lawful manner in accordance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA 2018)
- The EU General Data Protection Regulation (EU GDPR 2016/679) â€“ where applicable for EEA data subjects
- The Privacy and Electronic Communications Regulations 2003 (PECR)
- Any other applicable national or international data protection legislation

2. Who We Are â€“ Data Controller Details

Fitzrovia IT Limited is the data controller for the personal data described in this policy. This means we are responsible for determining how and why your personal data is processed.

Category	**Details**
Company Name	Fitzrovia IT Limited
Registered Address	1st Floor Arthur Stanley House, 40-50 Tottenham Street, London, United Kingdom, W1T 4RN
Company Number	03720812
ICO Registration No	Z2858261 â€“ registered with the Information Commissioner's Office
General Privacy Enquiries	privacy@fitzroviait.com
Website	www.fitzroviait.com

3. Personal Data We Collect

"Personal data" means any information that identifies, or can be used to identify, a living individual (a "data subject"). We collect and process the following categories of personal data:

3.1 Identity & Contact Data

- Full name, title, date of birth, gender
- Postal address, email address, telephone number(s)
- Username, password (hashed), and similar account credentials
- Photographic identification where required by law or for verification purposes

3.2 Financial & Transaction Data

- Bank account details, payment card information (tokenised via our payment provider â€“ we do not store raw card data)
- Transaction history, invoices, receipts, and billing records
- Credit or debit card expiry dates (partial â€“ last 4 digits only)
- Information about purchases, orders, and subscriptions

3.3 Technical & Usage Data

- IP address, device identifiers, browser type and version
- Operating system, referring/exit pages, time zone and location
- Cookie identifiers and similar tracking technologies (see Section 14)
- Pages viewed, links clicked, session duration, and other interaction data
- Log files and error reports

3.4 Profile & Preference Data

- Interests, preferences, and settings you provide or we infer from your activity
- Survey responses, competition entries, and feedback
- Wishlist, saved items, and product history
- Marketing and communication preferences

3.5 Communications Data

- Correspondence sent to or received from us (email, live chat, postal letters)
- Telephone call recordings (where applicable and notified to you)
- Social media interactions where you tag, message, or contact us through social platforms

3.6 Employment & Recruitment Data (Job Applicants & Employees)

- CV / curriculum vitae, cover letter, and application form
- Employment history, qualifications, and references
- Right-to-work documents and identity checks
- Performance reviews, disciplinary records (employees)
- Emergency contact details (employees)
- Bank details for payroll; NI number; tax information (employees)

3.7 Special Categories of Personal Data

Warning â€“ Sensitive Data

The following categories of personal data are afforded enhanced protection under UK/EU GDPR. We only process these data where a specific condition under Article 9 UK/EU GDPR applies and we have documented our lawful basis.

- Health or medical information (e.g. for accessibility adjustments or absence management)
- Racial or ethnic origin (where required for equality monitoring)
- Religious or philosophical beliefs (where disclosed voluntarily)
- Criminal convictions and offences data (where legally required, e.g. DBS checks)
- Biometric data used for identification (e.g. facial recognition) â€“ only where explicitly consented

We will never collect special-category data unless there is a clear and documented lawful basis and, where required, explicit consent.

3.8 Data We Receive from Third Parties

- Analytics providers (e.g. HubSpot)
- Advertising partners and social media platforms
- Credit reference agencies, fraud prevention agencies
- Publicly available registers (e.g. Companies House, electoral roll)
- Business information providers (e.g. LinkedIn,)

4. How We Collect Personal Data

We collect personal data through the following means:

Collection Method	Examples	Data Collected
Direct interaction	Registration forms, checkout, contact forms, phone calls, email	Identity, contact, financial
Automated technologies	Cookies, web beacons, pixels, server logs	Technical, usage, profile
Third-party sources	Analytics providers, social platforms, data brokers, partners	Identity, contact, technical
Publicly available sources	Companies House, LinkedIn, news articles	Identity, contact, professional
Referrals	Existing customers or partners who refer you to us	Identity, contact
Offline methods	Business cards, trade shows, postal correspondence	Identity, contact

5. Legal Bases for Processing Personal Data

We only process your personal data where we have a valid legal basis under Article 6 (and, for special-category data, Article 9) of the UK GDPR / EU GDPR. The legal bases we rely on are:

Legal Basis	When We Rely on It	Examples
Contract (Art. 6(1)(b))	Processing is necessary to perform a contract with you or take steps at your request before entering a contract	Processing orders, managing your account, delivering services
Legal Obligation (Art. 6(1)(c))	Processing is necessary to comply with a legal obligation	Tax records, anti-money laundering checks, safeguarding obligations
Legitimate Interests (Art.	Processing is necessary for our legitimate interests or those of a third party, and not overridden by	Fraud prevention, network security, direct marketing to existing customers, business

6(1)(f))	your rights	analytics
Consent (Art. 6(1)(a))	You have given clear, specific, informed, and unambiguous consent	Email marketing to prospects, non-essential cookies, processing special-category data
Vital Interests (Art. 6(1)(d))	Processing is necessary to protect the vital interests of you or another person	Medical emergencies
Public Task (Art. 6(1)(e))	Processing is necessary for a task in the public interest or for official authority	Where we are required to assist public authorities

Where we rely on legitimate interests as our legal basis, we conduct and document a Legitimate Interests Assessment (LIA) to ensure that our interests are not outweighed by your rights and freedoms.

Where we rely on consent, you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

6. How We Use Your Personal Data

We use your personal data for the following purposes:

6.1 Providing and Managing Our Services

- To create, manage, and administer your account
- To process orders, transactions, and payments
- To deliver goods, services, and digital content you have purchased or requested
- To handle returns, refunds, and complaints
- To provide customer support and respond to your enquiries

6.2 Legal and Regulatory Compliance

- To comply with applicable laws, regulations, and regulatory guidance
- To meet anti-money laundering (AML) and Know Your Customer (KYC) obligations
- To respond to lawful requests from law enforcement or regulatory authorities
- To maintain statutory records including tax and accounting records
- To conduct identity and credit checks where required

6.3 Security and Fraud Prevention

- To protect our business and customers from fraudulent, abusive, or unlawful activity
- To monitor and investigate suspicious transactions or behaviour
- To maintain the security and integrity of our IT systems and websites
- To verify your identity when you contact us

6.4 Marketing and Communications

- To send you promotional offers, newsletters, and marketing communications where you have consented or where we have a legitimate interest as an existing customer (subject to your right to opt out)
- To personalise content, recommendations, and advertisements
- To measure the effectiveness of our marketing campaigns
- To conduct market research, surveys, and product feedback exercises

Your Right to Opt Out

You may opt out of marketing communications at any time by clicking the 'unsubscribe' link in any email, by contacting us at privacy@fitzroviait.com, or by updating your preferences in your account. Opting out of marketing does not affect service-related communications necessary to manage your account.

6.5 Business Operations and Analytics

- To analyse how our products and services are used in order to improve them
- To conduct internal reporting, auditing, and performance monitoring
- To manage supplier and partner relationships
- To support business continuity, disaster recovery, and IT management
- To facilitate corporate transactions such as mergers, acquisitions, or restructuring

6.6 Recruitment and Human Resources

- To assess job applications and make hiring decisions
- To manage employee records, payroll, benefits, and performance
- To carry out right-to-work checks and background screening
- To comply with health and safety and employment law obligations

7. Sharing Your Personal Data

We do not sell your personal data to third parties. We may share your personal data with the following categories of recipients, and only to the extent necessary:

Recipient Category	Purpose	Legal Basis
Payment processors (e.g. Stripe, PayPal)	Processing transactions securely	Contract
Cloud hosting & IT service providers	Storing data; operating our systems	Legitimate interests / Contract
Analytics providers (e.g. HubSpot)	Understanding website usage	Consent / Legitimate interests
Email service providers (e.g. Microsoft 365)	Sending transactional & marketing email	Contract / Consent
Customer support platforms	Managing support tickets and communications	Contract / Legitimate interests
Fraud & credit reference agencies	Identity verification; fraud prevention	Legal obligation / Legitimate interests
Professional advisers (legal, audit, tax)	Legal, financial, and compliance advice	Legitimate interests / Legal obligation
Regulatory & law enforcement bodies	Compliance with legal obligations	Legal obligation
Group companies / subsidiaries	Internal administration, shared services	Legitimate interests
Business purchasers	In the event of a sale, merger, or acquisition	Legitimate interests

All third parties with whom we share personal data are required to have appropriate data protection measures in place and to process your data only in accordance with our instructions. Where we use third-party processors, we enter into data processing agreements (DPAs) compliant with Article 28 UK/EU GDPR.

8. International Transfers of Personal Data

Some of our service providers and partners are located outside the United Kingdom (UK) or the European Economic Area (EEA). Where we transfer personal data internationally, we ensure appropriate safeguards are in place as required by UK GDPR Chapter V and EU GDPR Chapter V.

8.1 Transfers from the UK

For transfers of personal data from the UK to countries outside the UK, we rely on one or more of the following mechanisms:

- UK Adequacy Regulations â€“ transfers to countries granted adequacy status by the UK Secretary of State
- International Data Transfer Agreements (IDTAs) â€“ the UK equivalent of Standard Contractual Clauses
- UK Binding Corporate Rules (BCRs) â€“ where approved by the ICO
- Derogations under Article 49 UK GDPR â€“ in limited circumstances

8.2 Transfers from the EEA

For transfers of personal data from the EEA to third countries, we rely on:

- EU Adequacy Decisions issued by the European Commission
- Standard Contractual Clauses (SCCs) adopted by the European Commission
- Binding Corporate Rules (BCRs) approved by a supervisory authority
- Appropriate derogations under Article 49 EU GDPR

You may request a copy of the relevant transfer mechanism by contacting us at privacy@fitzroviait.com.

9. Data Retention

We retain personal data only for as long as is necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or regulatory requirements. Our retention periods are set out in our Data Retention Schedule, a summary of which is provided below:

Data Category	**Retention Period**	**Reason**
Customer account data	Duration of relationship + 6 years	Contract; statutory limitation period
Financial & transaction records	7 years from end of financial year	UK HMRC / tax requirements
Marketing consent records	Until consent withdrawn + 1 year	Accountability; PECR compliance

Website analytics (cookies)	Up to 24 months (see cookie policy)	Legitimate interests
Customer service communications	3 years from last interaction	Legitimate interests; dispute resolution
Job applications (unsuccessful)	6 months from notification of outcome	Recruitment; potential re-application
Employee records	Duration of employment + 6 years	Employment law; tax obligations
CCTV footage (if applicable)	31 days unless subject to investigation	Security; legal proceedings
Call recordings (if applicable)	6 months (or up to 6 years if dispute)	Quality assurance; legal proceedings
Fraud prevention data	Up to 6 years	Legal obligation; fraud prevention

Where personal data is no longer required, we securely delete or anonymise it in accordance with our Data Destruction Policy. Where anonymisation is not possible, we implement restricted access and storage controls.

10. Your Data Subject Rights

Under UK GDPR and EU GDPR, you have the following rights in relation to your personal data. We will respond to all valid requests within one calendar month (extendable by two further months for complex or numerous requests, with notice):

Category	**Details**
Right of Access (Art. 15)	You have the right to obtain a copy of your personal data and supplementary information about how we process it (a 'Subject Access Request' or SAR). We may charge a reasonable fee or refuse manifestly unfounded or excessive requests.
Right to Rectification (Art. 16)	You have the right to require us to correct inaccurate or incomplete personal data we hold about you without undue delay.
Right to Erasure (Art. 17)	Also known as the 'right to be forgotten'. You may request deletion of your personal data where: it is no longer necessary for the purpose it was collected; you withdraw consent; you object and we have no overriding legitimate interests; the data has been unlawfully processed; or deletion is required to comply with a legal obligation. Exceptions apply (e.g. where data must be retained

	for legal compliance).
Right to Restriction of Processing (Art. 18)	You may request that we restrict processing of your personal data in certain circumstances â€“ for example, while accuracy is contested, or while we assess an objection.
Right to Data Portability (Art. 20)	Where processing is based on consent or contract and is carried out by automated means, you have the right to receive your personal data in a structured, commonly used, machine-readable format and to transmit it to another controller.
Right to Object (Art. 21)	You have the right to object to processing based on legitimate interests (including profiling) and to processing for direct marketing purposes. We will cease such processing unless we have compelling legitimate grounds that override your interests, rights, and freedoms.
Rights re Automated Decision-Making & Profiling (Art. 22)	You have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal or similarly significant effects. We will inform you if we use such processing and provide a mechanism for human review.
Right to Withdraw Consent (Art. 7(3))	Where we rely on consent as our legal basis, you may withdraw that consent at any time without affecting the lawfulness of prior processing. Withdrawing consent will not affect processing based on other legal bases.
Right to Lodge a Complaint	You have the right to lodge a complaint with the relevant supervisory authority: UK: Information Commissioner's Office (ICO) â€“ www.ico.org.uk â€“ 0303 123 1113 EEA: Your local data protection authority (see www.edpb.europa.eu for a list of EU supervisory authorities).

How to Exercise Your Rights

To exercise any of your data subject rights, please email us on privacy@fitzroviait.com.We may need to verify your identity before processing your request. We will not charge a fee for exercising your rights unless the request is manifestly unfounded, excessive, or repetitive.

11. Data Security

We take the security of your personal data seriously and have implemented appropriate technical and organisational measures (TOMs) to protect it against unauthorised access, accidental loss, destruction, or damage. These include, but are not limited to:

11.1 Technical Measures

- Encryption of personal data in transit (TLS/SSL) and at rest (AES-256)

- Multi-factor authentication (MFA) for access to systems holding personal data
- Firewalls, intrusion detection systems, and endpoint security controls
- Regular penetration testing and vulnerability assessments
- Secure software development lifecycle (SSDLC) practices
- Access controls based on the principle of least privilege
- Regular data backups with encrypted off-site storage

11.2 Organisational Measures

- Data protection training for all staff with access to personal data
- Internal data protection policies, procedures, and a Data Retention Schedule
- Data processing agreements (DPAs) with all sub-processors
- Regular internal audits and third-party assessments
- A documented Incident Response Plan
- Privacy by design and by default principles embedded in new projects and systems

Despite these measures, no transmission over the internet or electronic storage method is 100% secure. In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the relevant supervisory authority within 72 hours and, where required, notify affected individuals without undue delay, in accordance with Article 33 and 34 UK/EU GDPR.

12. Data Protection by Design and by Default

We implement data protection by design and by default in accordance with Article 25 UK/EU GDPR. This means:

- We consider data protection implications from the outset of any new project, product, or process
- We conduct Data Protection Impact Assessments (DPIAs) for processing activities likely to result in high risk to individuals' rights and freedoms, including large-scale processing of special-category data, systematic monitoring of publicly accessible areas, and use of new technologies
- We minimise the personal data we collect to that which is strictly necessary (data minimisation principle)
- We limit access to personal data to those who need it (need-to-know basis)
- We configure systems and services with privacy-protective settings as the default
- We regularly review and update our data protection practices as technologies and risks evolve

13. Cookies and Tracking Technologies

We use cookies and similar tracking technologies on our website(s). A cookie is a small text file placed on your device when you visit a website. We use the following categories of cookies:

Cookie Type	Purpose	Consent Required?
Strictly Necessary	Essential for the website to function (e.g. session management, security, load balancing)	No (exempt under PECR)
Functional / Preference	Remembering your preferences, language settings, and login details	Yes
Analytics / Performance	Understanding how visitors use our site (e.g. HubSpot)	Yes
Marketing / Targeting	Serving relevant advertisements; remarketing; tracking conversions	Yes
Social Media	Enabling social sharing buttons; embedding social media content	Yes

On your first visit, you will be presented with a Cookie Consent Banner through which you can accept, reject, or manage your cookie preferences. You can also manage cookies through your browser settings; however, disabling certain cookies may affect website functionality.

14. Profiling and Automated Decision-Making

We may use automated processing, including profiling, to analyse your personal data to assess and predict certain personal preferences or characteristics. Where such processing produces legal or similarly significant effects on you, we will ensure:

- You are informed of the logic involved and the significance and envisaged consequences of the processing
- You have the right to obtain human intervention, express your point of view, and contest the decision
- We do not make solely automated decisions based on special-category data unless specific conditions under Article 22(4) UK/EU GDPR are met

Examples of automated processing we may carry out include: fraud scoring, credit risk assessment (where applicable), personalised product or content recommendations, and segmentation for marketing communications.

15. Direct Marketing

We may send you direct marketing communications about our products, services, and offers by:

- Email â€“ subject to your consent or, for existing customers, on the basis of legitimate interests (soft opt-in) in accordance with PECR Regulation 22
- SMS / text message â€“ only with your explicit consent
- Post â€“ on the basis of legitimate interests, unless you object
- Telephone â€“ in accordance with TPS (Telephone Preference Service) and CTPS (Corporate TPS) screening

You have the right to object to direct marketing at any time, without giving a reason. You can unsubscribe from email marketing using the link provided in every email, or by contacting privacy@fitzroviait.com. We will action your request within 10 working days.

16. Third-Party Websites and Links

Our website may contain links to third-party websites, plugins, 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. We encourage you to read the privacy policy of every website you visit.

17. Employee and Staff Privacy

This policy applies to all personal data processed in respect of our employees, workers, and contractors. A separate Employee Privacy Notice is provided to all staff at commencement of employment / engagement, setting out in full how we process employee personal data, including:

- Payroll, benefits, and pension administration
- Performance management and disciplinary procedures
- Monitoring of company devices, email, and internet use (where applicable)
- Occupational health and absence management
- CCTV and access control systems (where applicable)
- Training records and professional development

Where we monitor employees' use of company equipment or communications, we do so only to the extent necessary and proportionate, and employees are informed of this monitoring through our Employee Privacy Notice and Acceptable Use Policy.

18. Records of Processing Activities (ROPA)

In accordance with Article 30 UK GDPR / EU GDPR, we maintain a written Record of Processing Activities (ROPA) covering all processing operations carried out on personal data. Our ROPA includes:

- The name and contact details of the controller, joint controller(s), and DPO
- The purposes of processing
- A description of categories of data subjects and personal data
- Categories of recipients
- Details of international transfers and applicable safeguards
- Retention periods and data deletion schedules
- A description of technical and organisational security measures

Our ROPA is available to the ICO and relevant supervisory authorities on request.

19. Personal Data Breach Management

In the event of a personal data breach, we follow our documented Incident Response Procedure:

1. Detect and contain the breach as quickly as possible
2. Assess the risk to individuals' rights and freedoms
3. Notify the ICO (and, where applicable, EU supervisory authorities) within 72 hours of becoming aware of a breach likely to result in a risk to individuals â€“ in accordance with Article 33 UK/EU GDPR
4. Notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms â€“ in accordance with Article 34 UK/EU GDPR
5. Document all breaches (including those not reported) in our Breach Register
6. Review and remediate root cause to prevent recurrence

If you suspect or discover a personal data breach involving your data, please contact us immediately at privacy@fitzroviait.com.

20. Changes to This Privacy Policy

We review and update this Privacy Policy periodically to reflect changes in our processing activities, legal requirements, or guidance from regulatory authorities. We will:

- Update the 'Last Updated' date at the top of this policy
- Post the revised policy on our website at https://fitzroviait.com/privacy-policy-1
- Where changes are material, notify you by email or by prominent notice on our website prior to the change taking effect

We encourage you to review this policy regularly. Your continued use of our services after any changes signifies your acknowledgement of the updated policy.

21. Contact Us and How to Complain

If you have any questions, concerns, or requests regarding this Privacy Policy or our data processing activities, please contact us:

Category	**Details**
Privacy Team	privacy@fitzroviait.com
Website	https://fitzroviait.com/privacy-policy-1

21.1 Raising a Complaint with Us

We take complaints very seriously. If you are unhappy with how we have handled your personal data, please contact us in the first instance and we will work to resolve your concern within 30 days.

21.2 Right to Complain to a Supervisory Authority

You have the right to lodge a complaint directly with the relevant supervisory authority at any time:

Category	**Details**

UK â€“ Information Commissioner's Office (ICO)	www.ico.org.uk ICO Helpline: 0303 123 1113
Full list of EU Supervisory Authorities	www.edpb.europa.eu

Annex A â€“ Key Definitions

For the purposes of this Privacy Policy, the following terms have the meanings set out below:

Category	**Details**
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'). Article 4(1) UK/EU GDPR.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a natural person's sex life or sexual orientation. Article 9 UK/EU GDPR.
Processing	Any operation performed on personal data, including collection, recording, storage, use, disclosure, erasure, and destruction. Article 4(2) UK/EU GDPR.
Controller	The natural or legal person that determines the purposes and means of processing personal data. Article 4(7) UK/EU GDPR.
Processor	A natural or legal person that processes personal data on behalf of the controller. Article 4(8) UK/EU GDPR.
Data Subject	The identified or identifiable natural person to whom personal data relates. Article 4(1) UK/EU GDPR.
Consent	Freely given, specific, informed, and unambiguous indication of the data subject's agreement to processing. Article 4(11) UK/EU GDPR.
Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Article 4(12) UK/EU GDPR.
DPA 2018	The Data Protection Act 2018, which supplements and gives effect to the UK GDPR in domestic law.
ICO	The Information Commissioner's Office â€“ the UK's independent data protection supervisory authority.

PECR	The Privacy and Electronic Communications Regulations 2003, governing electronic marketing and the use of cookies.
UK GDPR	The retained EU law version of the General Data Protection Regulation as it forms part of UK domestic law by virtue of the European Union (Withdrawal) Act 2018.
EU GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.
DPIA	Data Protection Impact Assessment â€“ a process to identify and mitigate data protection risks before a new processing activity begins. Article 35 UK/EU GDPR.
LIA	Legitimate Interests Assessment â€“ a three-part test to assess whether processing on the basis of legitimate interests is lawful.
IDTA	International Data Transfer Agreement â€“ the UK mechanism for lawful transfers of personal data to third countries.
SCCs	Standard Contractual Clauses â€“ the EU mechanism for lawful international transfers of personal data adopted by the European Commission.