

Data Protection Privacy Notice

Royce Peeling Green Limited and RPG Services Limited

Publication-ready draft

Last updated: 1 July 2026

Royce Peeling Green Limited and RPG Services Limited are committed to protecting your personal information and respecting your privacy. This privacy notice explains how we collect, use, store, record, monitor and share personal information when we provide accountancy, tax, audit, payroll, business advisory, insolvency, company secretarial, support and related professional services.

In this notice, “RPG”, “we”, “us” and “our” means Royce Peeling Green Limited and RPG Services Limited, unless the context requires otherwise. This notice applies to clients, prospective clients, individuals connected with our clients, suppliers, professional contacts, website users and other people whose personal information we process in the course of our work.

This notice is intended to be read alongside our engagement letters, terms of business, cookie notice, website terms and any service-specific privacy information we provide to you.

1. Who is responsible for your personal information?

The relevant RPG entity providing services to you will usually be the controller of your personal information. This means that we decide why and how your personal information is used.

Our contact details are:

Royce Peeling Green Limited and RPG Services Limited
The Copper Room, Deva Centre, Trinity Way, Manchester, M3 7BG
Telephone: 0161 608 0000
Email: info@rpg.co.uk
Website: www.rpg.co.uk

If you have any questions about this notice or how we use your personal information, please contact us using the details above.

2. How we collect personal information

We may collect personal information directly from you when you contact us, engage us, complete forms, provide documents, attend meetings, use our website, use our portals or communicate with us.

We may also collect personal information from your employer, company, partnership, fellow directors, shareholders, trustees, beneficiaries, family members, representatives, HMRC, Companies House, the Insolvency Service, courts, regulators, banks, pension providers, insurers, software providers, professional advisers, public registers, anti-money laundering systems, identity verification providers, fraud prevention providers and other third parties.

3. What personal information we collect

The personal information we collect will depend on the services we provide and your relationship with us. It may include contact details; identification information; tax references; National Insurance numbers; bank details; financial records; payroll data; accounting records; business records; directorship, shareholding, partnership, trust or estate information; identity documents; AML records; sanctions, PEP and fraud-prevention checks; correspondence; telephone calls; SMS messages; WhatsApp messages; meeting recordings; online meeting records; meeting notes; transcripts; website and technical information; complaints, queries, instructions, consents, preferences and service history.

In some circumstances, we may process special category personal information, such as health information, trade union information, biometric information used for identification, or information revealing racial or ethnic origin, religious or philosophical beliefs or other sensitive matters, where this is necessary for the services we provide or where the law allows us to do so.

We may also process criminal offence, sanctions, fraud prevention or regulatory information where this is necessary for anti-money laundering, fraud prevention, insolvency, regulatory, legal or risk-management purposes.

4. How and why we use personal information

We use personal information to provide professional services, comply with legal, regulatory and professional obligations, verify identity, prevent financial crime, communicate with you, manage our client relationships, record and monitor communications, administer our business, manage risk, improve service quality, deal with complaints and protect our systems, clients, colleagues and firm.

5. Lawful bases for processing

The lawful basis we rely on will depend on the context and the purpose of the processing. The main bases we expect to rely on are set out below. Where we process special category data or criminal offence data, we will also identify and rely on an additional condition required by data protection law.

Purpose	Types of personal information	Likely lawful basis
Providing professional services	Client records, financial data, tax data, payroll data, business records, correspondence and engagement information	Contract; legitimate interests where information relates to individuals connected with a client
Legal, regulatory and professional compliance	Identity documents, AML records, tax records, audit records, insolvency records, statutory records and professional file records	Legal obligation; legitimate interests
Anti-money laundering, sanctions and fraud prevention	Identity evidence, proof of address, source of funds/wealth information, sanctions/PEP outcomes and fraud-prevention information	Legal obligation; legitimate interests
Communications and relationship management	Contact details, email, telephone, SMS, WhatsApp, portal, meeting and correspondence records	Contract; legitimate interests
Recording and monitoring communications	Telephone recordings, meeting recordings, transcripts, SMS, WhatsApp, emails, notes, summaries and related metadata	Contract; legal obligation; legitimate interests

Marketing and client updates	Contact details, preferences, service history and business relationship information	Legitimate interests or consent, depending on the communication and recipient
Complaints, claims and insurance	Matter records, correspondence, advice history, complaint records, call/meeting records and supporting documents	Legal obligation; legitimate interests
Business administration and security	System logs, access records, supplier records, audit trails, business continuity and cyber-security information	Legitimate interests; legal obligation

6. Recording and monitoring communications

To ensure we carry out your instructions accurately, to help us continually improve our service and in the interests of security, we will record and may monitor your telephone communications, meeting recordings, SMS or WhatsApp conversations with us.

We may also retain related emails, meeting notes, transcripts, summaries, online meeting records, chat records and other electronic communications. We use these records to confirm instructions, maintain accurate records, improve service quality, support training, monitor compliance, deal with queries or complaints, protect clients and colleagues, and meet legal, regulatory and professional obligations.

We may use approved technology tools to record, transcribe, summarise or manage communications. Any recordings, transcripts, summaries or AI-generated outputs are subject to review and must not be treated as formal written advice unless expressly confirmed by us in writing as our formal advice.

We will retain communication records in accordance with our retention policies and applicable legal or regulatory requirements. Copies may be available on request, subject to applicable law, confidentiality obligations, professional privilege, regulatory restrictions and the rights of other individuals.

7. Who we share personal information with

- HMRC, Companies House, the Insolvency Service, courts, law enforcement agencies, regulators and professional bodies;
- banks, payment providers, pension providers, insurers, payroll providers and other organisations involved in the services we provide;
- software providers, cloud service providers, IT support providers, cyber-security providers, document-management providers, identity verification providers, e-signature providers, data-hosting providers and communication platforms;
- subcontractors, consultants, professional advisers, insurers and other service providers who support our work;
- other members of the RPG group or associated entities where necessary for administration, service delivery, risk management or client service;
- third parties where you instruct us to share information or where disclosure is required or permitted by law.

We do not sell your personal information. Where we use third-party service providers to process personal information on our behalf, we require them to protect the information and use it only for the purposes for which it was provided.

8. International transfers

We usually process personal information in the United Kingdom. However, some systems, service providers or professional contacts may store, access or process personal information outside the United Kingdom. Where personal information is transferred outside the United Kingdom, we will take steps designed to ensure that it receives an appropriate level of protection. This may include relying on UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses, contractual protections, transfer risk assessments or other safeguards permitted by data protection law.

9. How long we keep personal information

We keep personal information only for as long as necessary for the purposes for which it was collected, including to provide services, maintain records, comply with legal and regulatory obligations, respond to questions or complaints, manage risk and defend legal claims. Retention periods vary depending on the type of information and the services provided. Professional records may need to be kept for several years after the end of our relationship with you because of legal, tax, regulatory, insurance, limitation and professional obligations. Where we no longer need personal information, we will securely delete, anonymise or restrict access to it, unless we are required or permitted to retain it.

10. How we protect personal information

We use appropriate technical and organisational measures to protect personal information against unauthorised access, loss, misuse, alteration or disclosure. These may include access controls, password protection, encryption, secure systems, staff confidentiality obligations, training, monitoring, backups, cyber-security tools and supplier due diligence. No method of transmission or storage is completely secure. You are responsible for keeping passwords, portal access details and authentication information confidential.

11. Your data protection rights

- request access to your personal information;
- request correction of inaccurate or incomplete information;
- request deletion of your information in certain circumstances;
- request restriction of processing in certain circumstances;
- object to processing in certain circumstances;
- request data portability in certain circumstances;
- withdraw consent where we rely on consent;
- object to direct marketing;
- challenge certain automated decisions, where applicable.

These rights are not absolute and may be subject to legal, regulatory, confidentiality, professional privilege or other restrictions. We may need to verify your identity before responding to a request.

12. Complaints

If you have concerns about how we handle your personal information, please contact us first so that we can try to resolve the issue. You also have the right to complain to the Information Commissioner's Office: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 0303 123 1113. Website: ico.org.uk/concerns.

13. Changes to this privacy notice

We keep this privacy notice under regular review and may update it from time to time. The latest version will be available on our website or on request.