

Privacy Notice

Last updated: September 2026

About this Privacy Notice

This notice is for Opus Advisory Group referred to as 'Opus' which also incorporates the entities listed on the Corporate Governance page of the firm's website:

<https://opusllp.com/about-us/corporate-governance-opus/>

These entities are collectively known as Opus.

Opus Advisory Group ("Opus", "we", "us" or "our") respects your privacy and is committed to protecting personal data.

This Privacy Notice explains how personal data may be collected, used, disclosed, retained and protected in connection with Opus' business and professional services. It also explains how personal data is handled where an Insolvency Practitioner working with Opus acts in a statutory or other formal appointment as an Office Holder.

Depending upon the circumstances, personal data may be processed in connection with:

- Restructuring and insolvency, including statutory Office Holder appointments
- Business advisory and turnaround services
- Forensic accounting and investigations
- Litigation and dispute support
- Corporate finance and related professional services
- Client and prospective client relationships
- Suppliers and professional advisers
- Marketing and business development
- Recruitment and employment-related activities
- Operation of our websites and online services
- Legal and regulatory obligations
- Administration and operation of our business

This Notice should be read alongside any more specific privacy information provided in relation to a particular engagement, appointment, jurisdiction or processing activity. Where an Office Holder is appointed, correspondence relating to the appointment will normally identify the relevant Office Holder or Office Holders.

Legal framework: Articles 5(1)(a), 12, 13 and 14 UK GDPR; Data Protection Act 2018 ("DPA 2018"), as amended including by the Data (Use and Access) Act 2025 ("DUAA 2025").

Who We Are and Who Is the Data Controller

Opus Advisory Group provides restructuring, insolvency, advisory, forensic and associated professional services.

For the purposes of UK data protection law, the identity of the Data Controller depends upon the circumstances and the legal or professional capacity in which personal data is processed.

Opus as Data Controller

Opus will normally act as Data Controller where it determines the purposes and means of processing, including in relation to its own clients, prospective clients, suppliers, personnel, recruitment, marketing, websites, business administration, compliance and other corporate activities.

There may also be circumstances in which Opus processes personal data on behalf of another Data Controller. Where Opus acts solely as a Data Processor, the relevant Data Controller is principally responsible for providing privacy information concerning that processing.

Office Holders as Data Controllers

An "Office Holder" is an Insolvency Practitioner appointed in a personal statutory or formal capacity, for example as a liquidator, trustee in bankruptcy, administrator, administrative receiver, nominee or supervisor of a voluntary arrangement, or another equivalent insolvency office.

Where an Office Holder determines the purposes and means of processing personal data in order to discharge the duties and functions of their appointment, the relevant Office Holder will be the Data Controller for that processing. Opus may provide the Office Holder with staff, systems, premises and administrative support, but this does not of itself make Opus the controller of personal data processed by the Office Holder in that statutory capacity.

The position can differ according to the type of appointment and the processing activity. For example, an administrator may act as agent of a company and the company may continue to be the controller for some processing undertaken in the ordinary course of its business, while the Office Holder may separately be a controller for processing undertaken for their own statutory duties. Where necessary, we will clarify the relevant controller in case-specific correspondence or privacy information.

If you are unsure which Opus entity or Office Holder is responsible for your personal data, please contact us using the details below.

Data Protection Contact

Email: dataprotection@opusllp.com

Postal address:

Opus Advisory Group

1 Radian Court, Knowlhill, Milton Keynes, Buckinghamshire, MK5 8PJ.

Data Protection Officer:

Colin Wilson – colin.wilson@opusllp.com

Legal framework: Articles 4(7), 13, 14, 24, 26 and 28 UK GDPR, as applicable.

When This Notice Applies to Office Holder Appointments

Where a person or business is subject to insolvency or similar proceedings, one or more Insolvency Practitioners may be appointed to realise or protect assets, investigate affairs, adjudicate claims, make distributions, report to creditors and regulators, and carry out other functions required by law. These activities are referred to in this Notice as "Insolvency Services".

Office Holder appointments may include, depending upon the jurisdiction and circumstances:

- Bankruptcy and individual voluntary arrangements
- Receivership and administrative receivership
- Administration
- Creditors' voluntary liquidation and compulsory liquidation
- Company voluntary arrangements
- Members' voluntary liquidation
- Trust deeds, sequestration or equivalent procedures
- Other court, creditor or statutory insolvency appointments

Office Holders process personal data only to the extent reasonably necessary for the performance, administration and record keeping of their appointment, the discharge of legal and regulatory duties, and related professional requirements. Where a data protection right conflicts with a statutory duty or a lawful exemption applies, the Office Holder may be unable to comply with the request in full. Any such restriction will be considered on its facts and explained where the law permits.

The Personal Data We May Process

The personal data processed depends upon the relationship, engagement or appointment concerned. It may include:

Category of Personal Data	What This Includes
Identity Data	Name, title, date of birth, identification documents, signatures, passport details, driving licence details, national insurance number and other identifiers
Contact Data	Home address, business address, email address, telephone numbers and other contact details
Professional and Employment Data	Employer, job title, employment history, professional qualifications, directorships, business interests, remuneration and employment records
Financial Data	Bank account information, assets, liabilities, income, expenditure, debts, taxation information, investments, payroll and pension information
Insolvency, Claims and Case Data	Directors, shareholders, employees, creditors, claimants, debtors, company records, proofs of debt, claims, investigations, transactions and case records
Family and Dependent Data	Names, dates of birth, relationships and information relevant to appointments, claims or investigations
Communications Data	Correspondence, emails, telephone communications, meeting records, enquiries and complaints
Technical and Website Data	IP address, browser information, device information, website usage data, cookies and access information
Marketing Data	Marketing preferences, communication preferences, event attendance, subscriptions and marketing engagement data

Special Category and Criminal Offence Data

Given the nature of some professional engagements and Office Holder appointments, Special Category Personal Data may occasionally be processed. This can include information concerning health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric information used for identification, or sex life or sexual orientation.

Information concerning criminal allegations, investigations, convictions, offences or related security measures may also be processed, particularly where relevant to forensic investigations, fraud, misconduct, sanctions, regulatory matters, director conduct, insolvency proceedings or legal claims.

Such information will only be processed where the law permits. Special Category Personal Data requires both an Article 6 lawful basis and an applicable condition under Article 9 UK GDPR. Where required, an appropriate condition under Schedule 1 DPA 2018 will also be identified. Criminal offence data will be processed in accordance with Article 10 UK GDPR and the applicable provisions of the DPA 2018. Where required, processing will be supported by an Appropriate Policy Document.

Legal framework: Articles 6, 9 and 10 UK GDPR; sections 10-11 and Schedule 1 DPA 2018.

How We Obtain Personal Data

Personal data may be obtained directly from you, including where you instruct or contact Opus or an Office Holder, correspond with us, submit information through a website or portal, make or pursue a claim, attend an event, subscribe to communications, apply for employment, supply goods or services, or otherwise interact with us.

Given the nature of our work, personal data is also frequently received from other sources, including:

- Clients and prospective clients
- Companies and their directors, officers, employees or agents
- Insolvent companies or individuals and their books and records
- Insolvency Practitioners and Office Holders
- Creditors, claimants and debtors
- Banks and financial institutions
- Professional advisers, solicitors, accountants and auditors
- Regulators, government departments and public authorities
- Law enforcement agencies, courts and tribunals
- Employers, insurers, suppliers, counterparties, witnesses and complainants
- Sanctions and financial crime screening providers
- Publicly accessible registers and records, including Companies House and court records
- News reports, websites and other publicly available sources
- Other parties connected with an engagement or appointment

Personal data remains subject to applicable data protection requirements merely because it has been obtained from a publicly available source.

Legal framework: Articles 5(1)(a), 6, 14 and 14(2)(f) UK GDPR.

Why We Use Personal Data and Our Lawful Bases

Personal data will only be processed where an appropriate lawful basis applies. Depending upon the circumstances, the purposes and lawful bases may include the following:

Providing Professional Services

To provide restructuring, insolvency, forensic, advisory and other professional services. Depending upon the circumstances, processing may be necessary for performance of a contract or pre-contractual steps (Article 6(1)(b)), compliance with legal obligations (Article 6(1)(c)), a recognised legitimate interest where the statutory conditions are met (Article 6(1)(ea)), or legitimate interests (Article 6(1)(f)).

Insolvency and Office Holder Functions

To undertake insolvency appointments, realise and protect assets, manage the affairs of an estate or company where relevant, investigate conduct and transactions, adjudicate claims, make distributions, report to creditors and authorities, maintain appointment records and discharge statutory or professional functions. Processing will commonly be necessary to comply with legal obligations (Article 6(1)(c)) and may also, where appropriate, rely upon recognised legitimate interests (Article 6(1)(ea)) or legitimate interests (Article 6(1)(f)). Relevant legislation may include the Insolvency Act 1986, Insolvency Rules 2016, Company Directors Disqualification Act 1986, Companies Act 2006 and other legislation or regulatory requirements applicable to the appointment.

Fraud, Financial Crime, AML and Sanctions

To prevent and detect fraud, undertake identity and anti-money laundering checks, conduct sanctions screening, investigate financial crime and comply with related regulatory or legal requirements. Depending upon the circumstances, we may rely upon legal obligation, recognised legitimate interests or legitimate interests. Relevant legislation may include the Proceeds of Crime Act 2002 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, where applicable.

Legal Claims and Disputes

To establish, exercise or defend legal claims, obtain legal advice, respond to proceedings or assist with disputes and litigation. Depending upon the circumstances, we may rely upon Articles 6(1)(c) or 6(1)(f) UK GDPR and, for Special Category Personal Data, Article 9(2)(f).

Regulatory and Professional Obligations

To meet legal, regulatory, professional, audit, insurance, compliance, reporting and record-keeping obligations. Lawful basis: Article 6(1)(c) and, where appropriate, Article 6(1)(f).

Client and Business Administration

To administer client relationships and engagements, issue and process invoices, manage suppliers and contracts, administer insurance, handle complaints, maintain business records and operate our business. Lawful bases may include Articles 6(1)(b), 6(1)(c) and/or 6(1)(f).

Security and Prevention of Misuse

To protect systems, personnel, premises, clients, estates, information and assets and to prevent or investigate misuse, fraud and security incidents. Lawful bases may include Articles 6(1)(c), 6(1)(ea) where applicable and/or 6(1)(f).

Recruitment

To manage recruitment and assess suitability for employment or engagement. Lawful bases may include Articles 6(1)(b), 6(1)(c) and/or 6(1)(f), with additional conditions where Special Category or criminal offence information is involved.

Marketing and Business Development

To use professional contact information for communications about services, events, publications and relevant business developments. Depending upon the circumstances, we may rely upon consent or legitimate interests. Electronic direct marketing will also be undertaken in accordance with PECR. You can opt out of marketing communications at any time.

Legal framework: Articles 5 and 6 UK GDPR; DPA 2018; PECR 2003; DUAA 2025; and applicable insolvency, company, financial crime and professional legislation.

Office Holder Processing - Typical Data, Purposes and Lawful Bases

The following table gives additional information about personal data commonly processed by an Office Holder. The exact data and purpose will depend upon the appointment and the individual's connection with it.

Category of personal data	Typical purpose	Typical lawful basis
Contact details	Identifying and communicating with directors, employees, creditors, claimants, debtors and other stakeholders; identifying assets; investigating pre-appointment conduct and transactions; agreeing or adjudicating claims; making distributions; and maintaining appointment records.	Commonly Article 6(1)(c) - legal obligation under applicable insolvency and related law. Article 6(1)(f) or 6(1)(ea) may apply to particular activities where appropriate.
Identity documents	Identity verification, AML or financial crime checks, sanctions screening, verification of claims or payment details, and appointment record keeping.	Commonly Article 6(1)(c) where required by applicable law or professional regulation; otherwise Article 6(1)(f) where necessary and proportionate.

Category of personal data	Typical purpose	Typical lawful basis
Family and dependant information	Asset enquiries, investigations, verification of relationships, claims and other matters relevant to the statutory appointment.	Commonly Article 6(1)(c), with additional Article 9 or Schedule 1 conditions where Special Category Data is involved.
Financial information	Identifying and realising assets, establishing liabilities, assessing claims, investigating transactions, payroll or pension matters, tax matters, source-of-funds checks, making distributions and administering the estate or appointment.	Commonly Article 6(1)(c); Article 6(1)(f) or 6(1)(ea) may also apply depending upon the activity.
Claims data	Receiving, verifying, adjudicating and paying claims made by employees, creditors or other claimants and keeping records of those decisions.	Commonly Article 6(1)(c) under applicable insolvency and related law.
Director/officer and conduct information	Investigating the affairs of a company or individual, transactions before appointment, director conduct, potential claims, misconduct, fraud or regulatory issues.	Commonly Article 6(1)(c); additional Article 9, Article 10 and DPA 2018 conditions apply where relevant.
Information from public sources	Sanctions and financial crime screening, director or asset investigations, verification of identity or addresses and other enquiries necessary for the appointment.	Commonly Article 6(1)(c), 6(1)(ea) or 6(1)(f), depending upon the legal duty and purpose.
Appointment and decision records	Documenting the Office Holder's decisions, actions, statutory reporting, professional compliance, claims adjudication, distributions, investigations and closure of the appointment.	Commonly Article 6(1)(c) and, where applicable, Article 6(1)(f).

Where a particular statutory duty, regulatory requirement or exemption applies, the Office Holder will assess the lawful basis and any additional conditions by reference to the specific processing activity and appointment. The table is not intended to imply that every category is processed in every case.

Legitimate Interests

Where Article 6(1)(f) is relied upon, legitimate interests may include operating and administering the business, providing and improving professional services, managing client and stakeholder

relationships, protecting businesses, estates, clients and systems, preventing and investigating fraud or misconduct, establishing and defending legal rights, maintaining appropriate professional records, managing risk, obtaining professional advice, business development and communicating with professional and business contacts.

Where required, we consider whether those interests are overridden by the interests, rights or freedoms of the individual.

Recognised Legitimate Interests

UK data protection law provides a lawful basis for certain recognised legitimate interests. Where appropriate, Article 6(1)(ea) UK GDPR may be relied upon where processing is necessary for a purpose satisfying a recognised legitimate interest condition in Annex 1 UK GDPR. Relevant circumstances may include certain processing necessary for preventing, detecting or investigating crime, safeguarding vulnerable individuals, responding to emergencies, or responding to requests made by organisations carrying out qualifying public tasks or official functions.

Where Special Category or criminal offence information is involved, the additional legal requirements applicable to that information must also be satisfied.

Legal framework: Article 6(1)(ea) and Annex 1 UK GDPR, as inserted by DUAA 2025.

Sharing Personal Data

Personal data may be shared where necessary and lawful with recipients such as:

- Other Opus entities and group companies
- The relevant Office Holder or joint Office Holders
- Clients, insolvent companies or individuals, creditors and creditor representatives
- Professional advisers, solicitors, accountants, auditors, agents and specialist consultants
- Payroll, employment rights, health and safety and other professional service providers
- Banks, financial institutions and payment providers
- Insurers
- Courts, tribunals, regulators, recognised professional bodies and government bodies
- Law enforcement agencies, HM Revenue & Customs and Companies House
- IT, telecommunications, cloud, hosting, archiving, document production and case-management providers
- Identity, AML, sanctions, conflicts and financial crime screening providers
- Contractors and consultants

- Prospective purchasers, bidders or advisers where an Office Holder is selling a business or assets, including associated databases or customer lists, subject to appropriate confidentiality and legal safeguards
- Other parties where disclosure is necessary for the relevant engagement, appointment, legal obligation or lawful exercise of professional functions

Where another organisation processes personal data on behalf of a controller, appropriate contractual and organisational safeguards will be used in accordance with Article 28 UK GDPR. Where information is shared between independent controllers, each organisation is responsible for its own compliance obligations.

Information may also be disclosed where required or permitted by law, regulation, court order, insolvency procedure or applicable professional obligation.

Legal framework: Articles 5, 6, 26, 28 and 32 UK GDPR.

International Transfers

Some service providers, professional relationships, group arrangements or appointment activities may involve personal data being accessed, stored or processed outside the United Kingdom.

Where this constitutes a restricted transfer under UK GDPR, an appropriate transfer mechanism will be used. Depending upon the circumstances, this may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, another safeguard permitted by Article 46 UK GDPR, or an applicable exception under Article 49 UK GDPR. Where required, the applicable transfer risk assessment or data protection test will also be undertaken.

For Office Holder appointments subject to the data protection law of another jurisdiction, additional local privacy information may be supplied where required. This may include information about the relevant local supervisory authority and any jurisdiction-specific rights or transfer safeguards.

Legal framework: Articles 44-49 UK GDPR; DPA 2018; DUAA 2025.

Data Security

Appropriate technical and organisational measures are maintained to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage,

alteration, disclosure or access. Access should be limited to personnel and authorised third parties who require it for legitimate business, professional or appointment purposes.

Security arrangements are reviewed having regard to the nature, scope, context and purposes of processing and the risks presented to individuals.

Legal framework: Articles 5(1)(f), 24, 25 and 32 UK GDPR.

How Long We Keep Personal Data

Personal data is retained only for as long as reasonably necessary for the purposes for which it is processed. The appropriate period depends upon the nature of the information and the circumstances in which it is held.

Relevant factors include statutory retention requirements, insolvency and company law, regulatory and professional obligations, contractual requirements, accounting and taxation requirements, limitation periods, actual or potential legal proceedings, complaints, insurance requirements, fraud and financial crime prevention, the establishment or defence of legal claims and legitimate operational requirements.

Office Holder records

For Office Holder appointments, retention periods may depend upon the type of record, the date the appointment ends, dissolution of the relevant company or estate, statutory and professional requirements, and any continuing litigation, complaint, regulatory or insurance need. Under the current Opus retention approach described for Office Holder appointments:

- Records relating to the operations of the insolvent company or individual are generally retained for the duration of the insolvency process and securely destroyed approximately 12 months after the Office Holder ceases to act or the dissolution of the company, if later, unless a longer period is required; and
- Other records generated by the Office Holder during the appointment are generally retained for the duration of the insolvency process and securely destroyed approximately seven years after the Office Holder ceases to act, unless a longer or shorter period is required by law, regulation, professional obligation, litigation hold or another justified purpose.

Where information no longer needs to identify an individual, it may be securely deleted or anonymised.

Legal framework: Articles 5(1)(c) and 5(1)(e) UK GDPR.

Your Data Protection Rights

Depending upon the circumstances and the lawful basis upon which personal data is processed, you may have the right to:

- **Be informed** - receive clear information about how your personal data is processed (Articles 12-14 UK GDPR).
- **Access your personal data** - request confirmation that personal data is being processed and obtain a copy of that data and associated information (Article 15).
- **Rectification** - ask for inaccurate personal data to be corrected or incomplete information completed (Article 16).
- **Erasure** - in certain circumstances, ask for personal data to be erased. This right is not absolute and may not apply where continued processing is required by law or necessary for another lawful purpose (Article 17).
- **Restriction** - in certain circumstances, request restriction of processing (Article 18).
- **Data portability** - in applicable circumstances, receive personal data you provided in a structured, commonly used and machine-readable format or request its transfer to another controller (Article 20).
- **Object** - in certain circumstances, object to processing based upon legitimate interests or another applicable ground. There is an absolute right to object to processing for direct marketing purposes (Article 21).
- **Withdraw consent** - where processing is based upon consent, withdraw that consent at any time. Withdrawal does not affect processing undertaken lawfully before withdrawal (Article 7(3)).

Rights are subject to the conditions and exemptions contained in UK GDPR and the DPA 2018. In particular, an Office Holder may be required to retain or use information in order to comply with insolvency legislation, court orders, statutory investigations, claims adjudication, reporting duties or other legal and professional obligations. Where this limits a request, the relevant controller will explain the position where it is lawful and appropriate to do so.

Exercising Your Rights

To exercise a right or raise a data protection query, please contact:

Email: dataprotection@opusllp.com

Where your request concerns an Office Holder appointment, please identify the relevant company, individual, estate and/or Office Holder if known. Requests received by Opus will be directed to the relevant controller where appropriate.

You do not normally need to pay a fee to exercise your rights. Sufficient information may be requested to verify your identity where this is necessary and proportionate, and we may ask for

information reasonably required to identify the personal data or processing activity concerned. We will respond within the periods prescribed by applicable data protection law. In certain circumstances the response period may be extended, in which case you will be informed.

Legal framework: Article 12 UK GDPR and DPA 2018.

Complaints

If you have concerns about the use of your personal data, we encourage you to contact us first so that the relevant controller has an opportunity to investigate and respond. Complaints concerning an Office Holder appointment will be considered in the context of the relevant appointment and controller responsibilities.

You can contact the Data Protection Officer at: dataprotection@opusllp.com.

You also have the right to complain to the UK's independent data protection regulator:

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Telephone: 0303 123 1113

Website: www.ico.org.uk

Nothing in this Notice affects your right to make a complaint to the ICO. Where an appointment is subject to another jurisdiction's data protection law, information about the relevant local supervisory authority may be provided separately.

Legal framework: Articles 13(2)(d), 14(2)(e) and 77 UK GDPR; DPA 2018.

Cookies and Website Technologies

Our website may use cookies and similar technologies for essential functionality, security, analytics and, where applicable, other purposes. Where consent is legally required before a cookie or similar technology is placed or accessed, consent will be obtained. Further information is available in our Cookie Notice.

Legal framework: UK GDPR; DPA 2018; Regulation 6 PECR 2003, as amended.

Automated Decision-Making

We do not currently make decisions about individuals which produce legal or similarly significant effects based solely upon automated processing unless there is an appropriate lawful basis and the safeguards required by law have been implemented. Office Holders do not currently use solely automated decision-making for the exercise of their statutory appointment functions.

If this changes, appropriate information will be provided concerning the processing, including meaningful information about the logic involved and the significance and envisaged consequences where required by law.

Legal framework: Article 22 UK GDPR, as amended by DUAA 2025.

Changes to this Privacy Notice

This Privacy Notice is kept under review and may be updated where services, processing activities, Office Holder practices, regulatory requirements or legal obligations change. The latest version will be published on the Opus website and the date at the beginning of this Notice will identify when it was last updated.

Where a change materially affects how personal data is processed, appropriate steps will be taken to bring the change to the attention of affected individuals.

This consolidated Privacy Notice was last reviewed in September 2026 and replaces the August 2026 general Privacy Notice and the separate Office Holder Privacy Notice for the matters covered here.

Legal framework: Articles 5(1)(a), 12, 13 and 14 UK GDPR.