Client Privacy Policy

June 2026



Omny Group
The Great Hall, Mount Pleasant Road, Tunbridge Wells, TN1 1QQ

Client Privacy Policy

Introduction

The Omny Group companies respect your privacy and are committed to protecting your personal information. This privacy notice contains important information on who we are and how and why we collect, store, use and share your personal information. It also tells you about your privacy rights, how the law protects you and how to contact us or supervisory authorities if you have a complaint.

Important Information and Who We Are

Purpose of this Privacy Policy

This privacy policy aims to give you information on how Omny Group companies collect and process personal information in accordance with the UK General Data Protection Regulations (UK GDPR).

It applies to all our current and former clients, whether personal or business.

It is important that you read this privacy policy together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you (or your employees, workers, contractors or other business contacts (together referred to as "*Individuals*"), so that you are aware of how and why we are using such information.

We take your privacy seriously and are committed to safeguarding your data in compliance with applicable regulations.

Controller

Omny Group is made up of different legal entities, details of which are in the Glossary below.

This privacy policy is issued on behalf of the Omny Group. When we mention Omny Group, "we", "us" or "our" in this privacy policy, we are referring to the relevant company in the Omny Group responsible for processing your data. Each group company is a data controller for their own client data where it determines the purposes for which, and the manner in which, any personal information is processed. Where a group company does not determine the purposes for which,

and the manner in which, any personal information is processed, it acts as a data processor.

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the data privacy manager using the details set out below.

Contact details

If you have any questions about this Client Privacy Policy or how we handle your personal information, please contact us at:

- Email: privacy@omnygroup.co.uk
- Phone: 08000 986 220
- Address: Omny Group, Third Floor, The Great Hall, Mount Pleasant, Tunbridge Wells, Kent TN1 1QQ

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance. We will acknowledge your complaint within 30 days of receipt. We will investigate and respond to your complaint fully as soon as practicable.

Changes to the Privacy Policy and Your Duty to Inform Us of Changes

We keep our privacy policy under regular review. This version was last updated in June 2026. We reserve the right to update this privacy policy at any time. The most current version is available on our website.

It is important that the personal information we hold about you and your Individuals is accurate and current. Please keep us informed if your or your Individuals personal information changes during your relationship with us.

Data Protection Principles

We will comply with data protection law. This says that the personal information we hold about you, your Individuals or Subjects must be:

- used lawfully, fairly and in a transparent way
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
- relevant to the purposes we have told you about and limited only to those purposes

- accurate and kept up to date
- kept only as long as necessary for the purposes we have told you about
- kept securely

The Kind of Information We Hold About You or Your Individuals

When we collect, use and are responsible for certain personal information about you, your Individuals and Subjects, we are subject to the UK General Data Protection Regulation (UK GDPR).

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal information which require a higher level of protection.

We may collect, use, store and transfer different kinds of personal information about you, Individuals, or the living persons that you may wish to contract with, that you wish us to advise you in relation to, or persons that you may have a dispute with ("Subjects"), which we have grouped together as follows:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, gender, national insurance number, copy of passport (including passport number) and driving licence (including licence number)
- **Contact Data** includes billing address, delivery address, email address and telephone numbers
- **Financial Data** includes bank account and payment card details. VAT number, tax status information, payroll records
- **Employment Data** includes employment records (including salary, annual leave, pension and benefits information, job titles, work history, working hours, training records and professional memberships), photographs and CCTV footage relevant to employment related matters
- **Advice Data** includes details of disputes, contracts, transactions or advice involving or relating to Subjects

We may also collect, store, and use the following "special categories" of more sensitive personal information:

- information about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions and trade union membership

- information about your health, including any medical condition, health and sickness records
- generic information and biometric data
- information about criminal convictions and offences

How is Client Personal Information Collected

We typically collect personal information about you, Individuals or Subjects when taking instructions or providing products or services to you, either directly from the Individual or Subject or sometimes from our own background checks. We may sometimes collect additional information from third parties and public sources including referrers, solicitors on the other side of the matter or transaction, other representatives of a business client, background check agencies, HM Land Registry, Companies House, client due diligence providers or credit reference agencies.

How We Use Information About You and Your Individuals

We will only use the personal information when the law allows us to. Most commonly, we will use personal information in the following circumstances:

- where we need to perform the contract we have entered into with you i.e. when providing products or services to you.
- where we need to comply with a legal obligation.
- where it is necessary for our legitimate interests (or those of a third party) and the individual's interests and fundamental rights do not override those interests.

We may also use personal information in the following situations which are likely to be rare:

- where we need to protect your interests (or someone else's interests)
- where it is needed in the public interest or for official purposes.

Situations in which We Will Use Your Personal Information

We need all categories of information in the list above (see The Kind of Information We Hold About You) primarily to allow us to provide products and services for you and to enable us to comply with legal obligations.

In some cases, we may use personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. These legitimate interests are to manage our relationship with you, determine our respective rights and obligations and to

properly conduct our business. There may be more limited circumstances where we process persona data pursuant to your consent or an Individual's or Subject's consent. The situations in which we will process personal information are:

- performing client instructions
- providing advice and services to you
- manging our relationship with you (including engagement letters, billing and billing management)
- complying with regulatory and legal obligations
- conducting conflict checks and anti-money laundering checks and screening for financial and other sanctions or embargoes
- processing special category data in connection with your instructions
- business continuity and operational reasons including ensuring business policies are adhered to, improving efficiency, training and quality control
- using contact details for marketing our services and our newsletter (provided the individual has had an opportunity to object and unsubscribe)
- to keep our records updated and to study how we provide our services and grow our business
- to establish, exercise or defend a legal claim (against us or you)
- complying with health and safety obligations
- to prevent fraud or other criminal offences
- credit reference checks via external credit reference agencies and to recover debts and involve debt collection agencies
- to ensure network and information security, including preventing unauthorised access to our computer systems and preventing malicious software distribution
- to conduct data analytics studies to review and better understand client retention and attrition rates
- external audits and quality checks e.g. for the Law Society, Chambers, The Legal 500 accreditation auditing of our accounts
- insurance related matters
- to respond to any complaints we may receive from you or a third party
- to consider and respond to any applications for jobs submitted through our website

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of personal information depending on the specific purpose for which we are using personal information.

If You Fail to Provide Personal Information

Where we need to collect personal information by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

Change of Purpose

We will only use your or your Individuals' personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Disclosures of Personal Information

We may share your personal information with the parties set out below for the purposes set out above:

- companies within the Omny Group
- third parties we use to help deliver our services to you, e.g. service providers acting as processors in the UK, the EEA and the USA who provide our case management and finance system, IT and systems administration service providers including cloud service providers such as data storage platforms, shared service centres and financial institutions in connection with invoicing and payments
- third party external advisors or experts engaged in the course of providing services to you, e.g. barristers, tax advisors, technology service providers such as eDiscovery and document review platforms, occupational health advisers
- HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the UK who require reporting of processing activities in certain circumstances

- companies providing services for money laundering checks, sanction and PEP checks and other crime prevention purposes and companies providing similar services, including financial institutions and credit reference agencies
- other third parties we use to help promote our business, e.g. marketing agencies, Chambers and Legal 500
- third parties approved by you, e.g. social media sites you choose to link your account to or third-party payment providers
- our insurers and brokers
- our banks

We require all third parties to respect the security of personal information and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal information for their own purposes and only permit them to process your personal information for specified purposes and in accordance with our instructions. We ensure all outsourcing providers operate under service agreements that are consistent with our legal and professional obligations, including in relation to confidentiality.

We may share personal information with other third parties, for example in the context of the possible sale, merger or restructuring of our business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share personal information with the other parties if and to the extent required under the terms of the transaction.

We or the third parties mentioned above may occasionally also share personal information with:

- our, and their, external auditors, e.g. in relation to the audit of our accounts, in which case the recipient of the information will be bound by confidentiality obligations
- our and their professional advisors (such as lawyers), in which case the recipient of the information will be bound by confidentiality obligations
- law enforcement agencies, courts, tribunals and regulatory bodies to comply with our or their legal and regulatory obligations

How We Use Particularly Sensitive Personal Information

"Special Categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- in limited circumstances with your explicit written consent
- where we need to carry out our legal obligations
- where it is needed in the public interest, such as for equal opportunities monitoring
- where it is needed to assess your capacity on health grounds the delivery of our services

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your or your Individuals' interests (or someone else's interests) and you are not capable of giving or procuring consent, or where you or your Individuals have already made the information public. We may also process such information in the course of legitimate business activities with the appropriate safeguards.

We will use your or your Individuals' particularly sensitive personal information in the following ways:

- we will use information to comply with applicable laws
- we will use information about your physical or mental health, or disability status, to ensure we give the correct advice in delivering our services
- we will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to provide correct advice in delivery our services

We do not need your consent if we use special categories of your or your Individuals' personal information for the establishment, exercise or defence of legal claims or to exercise specific rights pursuant to applicable law. In limited circumstances, we may approach you for written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you or your Individuals can carefully consider whether you or they wish to consent. You should be aware that it is not a condition of your retained services with us that you agree to procure any request for consent from us.

Information About Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your or Individuals' interests (or someone else's interests) and you or your Individuals are

not capable of giving consent, or where you or your Individuals have already made the information public.

We may also process such information in the course of legitimate business activities with the appropriate safeguards.

We do not envisage that we will hold much information about criminal convictions.

However, we will collect information about criminal convictions if it is appropriate given the nature of the services required and where we are legally able to do so. Where appropriate, we may be notified of such information directly by you in the course of taking your instructions.

Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in the following circumstances:

- where we have notified you of the decision and given you 21 days to request a reconsideration
- where it is necessary to provide services to you and appropriate measures are in place to safeguard your rights.
- in limited circumstances, with your or your Individuals' explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You and your Individuals will not be subject to decisions that will have a significant impact on you your them based solely on automated decision making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you or your Individuals using automated means, however we will notify you in writing if this position changes.

Use of New and Novel Technologies

We strive to be at the forefront of innovation, both when providing services or our clients, as well as ensuring that our processes are as efficient and cost-effective

as possible. To this end, we may occasionally adopt new technology tools. Such tools may leverage artificial intelligence or cloud-based technologies owned by third parties.

New technology tools may be used for the following purposes:

- to automate repetitive tasks
- to assist with our anti-money laundering (AML) and know your client (KYC) procedures
- to help manage emails, meetings and tasks
- to assist with reviews or large volumes of documents
- to generate machine translations
- to develop, test and train the tools themselves

Prior to the adoption of any tool which takes advantage of artificial intelligence or cloud-based functionality, we conduct an extensive due diligence process in line with industry best practice, including with reference to our internal data privacy policies and security procedures. This ensures that confidentiality, security and transparent, ethical use of new technologies are always prioritised. Where such tools are used as part of the provision of services to our clients, any outputs they generate will be vetted by appropriately qualified and experienced members of staff. Where necessary, we will seek client consent for the use of any tool which is used for client work outside of our normal business operations.

International Transfers

Some of our external third parties are based outside the UK so their processing of your personal information will involve a transfer of data outside the UK.

Whenever we transfer your personal information out of the UK, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- we will only transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal information.
- where we use certain service providers, we may use specific contracts approved for use in the UK which give personal information the same protection it has in the UK.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal information out of the UK.

Data Security

We have put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal information on our instructions, and they are subject to a duty of confidentiality. This does not apply to personal information shared with third parties on the other side of a legal matter or transaction, or to third parties where we have a legal obligation to do so (e.g. HM Revenue & Customs), who will themselves become a data controller under the UK GDPR and comply with data protection principles.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Data Retention

How Long Will You Use the Information For?

We will only retain personal information for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain personal information for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Omny Law are subject to a number of legal requirements, for example:

- Basic client details must be available many years into the future for conflict checks in accordance with our regulatory obligations (they must adhere to the Solicitors Regulatory Authority's Code of Conduct)
- Regulatory solicitors accounts rules oblige us to retain certain client account information for at least six years from the date of the last accounting entry

- The Money Laundering Regulations 2007 require that we retain evidence of identity for at least five years after the business relationship ends and that we retain details of a transaction for a five-year period from the date on which all activities taking place in the course of the transaction were completed.

In addition to obvious legal requirements, we must retain personal information for our own and our clients' legitimate interests:

- section 14B of the Limitation Act 1980 provides that a negligence claim will be time barred after 15 years from the date on which the act or omission constituting negligence occurred, even where the cause of action has not yet accrued. Therefore, the very latest point that an action in negligence is likely to be taken is at the end of that 15-year period and we may need applicable evidence from our files during that time in respect of that negligence, to establish, exercise or defend a legal claim, whether for our clients or ourselves.

Accordingly, we will need to retain client files, which will contain personal information, for potentially long periods of time before destruction although, in the vast majority of situations, we will not be using the personal information on them until the specific need arises.

Our general policy on file retention is to destroy our physical paper files after 15 years for Omny Law and the remainder of the Group unless we need to keep them longer to satisfy any other requirements. Electronic client files are currently stored indefinitely but where appropriate matter documents may be restricted, password protected or encrypted, accessible only with a password or electronic key under the control of designated staff or anonymised or pseudonymised 15 years after the closure of the matter.

Emails that may contain your personal information are also stored indefinitely but secured using a cloud-based archiving solution, which requires the mailbox user's identification and password. As emails are relevant to client files, the same retention reasons specified above apply.

As indicated above, in some circumstances we may anonymise personal information so that it can no longer be associated with you or your Individuals, in which case we may use such information without further notice to you, and we may also pseudonymise or encrypt personal information so that it can no longer be associated with you without implementing technical measures as is permitted under the UK GDPR.

Your Legal Rights

Under certain circumstances, you have rights under the data protection laws in relation to your personal information.

You have the right to:

Request access to your personal information (commonly known as a "Data Subject Access Request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

PLEASE NOTE: We can refuse to comply with a request where the personal information is subject to legal professional privilege. If applicable, this will be explained to you in the response that you receive.

Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you to be corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal information to comply with local law.

PLEASE NOTE: we can refuse to comply with a request where it needs to process information for the establishment, exercise or defence of legal claims or to comply with a legal obligation. If applicable, this will be explained to you in the response you receive.

Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal information for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

PLEASE NOTE: we may still need to continue to process data under applicable exemptions which include compelling legitimate grounds or for the

establishment, exercise or defence of legal claims. If applicable, this will be notified to you at the time of your objection.

Request restriction of processing of your personal information. This enables you to ask us to suspend the processing of your personal information in the following scenarios:

- if you want us to establish the data's accuracy.
- where our use of the data is unlawful, but you do not want us to erase it.
- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
- you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

PLEASE NOTE: even if processing is restricted, we may well need to continue to process the data under applicable exemptions which include the establishment, exercise or defence of legal claims. If applicable, this will be notified to you at the time of your request.

Request the transfer of your personal information to you or to a third party. We will provide to you, or a third party you have chosen, your personal information in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent. In circumstances where you or your Individuals may have provided consent to the collection, processing and transfer of personal information for specific purposes, that individual has the right to withdraw such consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact us at: privacy@omnygroup.co.uk or send a letter addressed to the address above under contact details.

No Fee Usually Required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What We May Need from You

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal information (or to exercise any of your other rights). This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time Limit to Respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Glossary

Lawful Basis

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal information for our legitimate interests. We do not use your personal information for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply With a Legal Obligation means processing your personal information where it is necessary for compliance with a legal obligation that we are subject to.

Omny Group

The Omny Group is made up of different legal entities being Omny Group Limited and the following subsidiaries which are listed below under their trading names:

Omny HR:

- Adastra HR Limited
- Aspiring HR Limited
- HR Revolution Limited
- HRR Solutions Limited
- Vero HR Limited

Omny Law:

- Outset Limited

Omny Benefits:

- Corinthian Benefits Consulting Limited
- Corinthian Affinity Solutions Limited

Omny Safety:

- Complete Health and Safety Limited
- Eyton Solutions Limited
- UK Health, Safety and Environmental Training Limited

Omny Personal Finance:

- Corinthian Benefits Consulting Limited