Third Party Privacy Policy

June 2026



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

Third Party 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 does not apply to our clients and our staff. We have separate privacy notices if you are a client or member of staff (our client privacy policy is also available on our website).

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 can be found here.

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 Third 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.

Who Are Third Parties for the Purposes of This Policy

Most of the personal information we collect and use is client data. A separate privacy notice details how we collect and use the data of our clients. We also collect and use personal information about our current and former staff and prospective candidates and there are also separate privacy notices for them.

In addition, we collect and use personal information of the following individuals ("you" for the purposes of this policy):

- Individuals connected with a matter or transaction we are advising a client on or have advised a client on, such as (but not limited to):
    - an individual our client has a legal dispute with
    - a witness or an expert involved in such a dispute
    - an individual our client is going into business with (e.g. a partner, director or shareholder)
    - an individual that is buying an asset from or is selling an asset to our client
    - another adviser or an expert to either (i) our client or (ii) the individual connected with a matter or transaction we are advising a client on or have advised a client on
    - representatives of a corporate entity connected with a matter or transaction we are advising a client or have advised a client on

who we will refer to collectively as a *matter data subject* in this policy.

- Possibly suppliers, or representatives of corporate suppliers of goods or services to us or our clients (including potential suppliers that have asked us to do something before entering into a supply contract).

Sometimes, if you are a *matter data subject*, we may only process your personal information on behalf of our clients. However, sometimes (given the advice we are providing clients), we are responsible for deciding how we hold and use personal information about you and when we act in the best interests of our clients.

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 versions is available on our website.

Data Protection Principles

We will comply with data protection law. This says that the personal information we hold about you 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

When we collect, use and are responsible for certain personal information about you, 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, 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 *matter data 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

In respect of *matter data subjects*, we typically collect personal information about you when taking instructions from our clients or dealing with a legal mater for them, either directly from our client or sometimes from our own background checks. We may sometimes collect additional information from your directly or 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.

We may collect additional information about you throughout the period of us acting for our client.

In respect of our suppliers (or representatives of suppliers), we may collect your personal information when negotiating the supply of goods or services from you (or the person you represent).

How We Use Information About You

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

- in respect of *matter data subjects* (i) where it is necessary for our clients' legitimate interests and your interests and fundamental rights do not override those interests; and (ii) where we need to comply with a legal obligation
- in respect of our suppliers (or representatives of suppliers) (i) where we need to perform the contract we have entered into with you; (ii) where it is necessary for our or our clients' legitimate interests and your interests and fundamental rights do not override those interests; and (iii) where we need to comply with a legal obligation

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.

Change of Purpose

We will only use your 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 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.

Situations in Which We Will Use Your Personal Information

In respect of *matter data subjects*, we need to use your personal information to comply with legal obligations and to pursue legitimate interests of our clients, provided your interests and fundamental rights do not override those interests. The situations in which we will process personal information this way are listed below:

- to progress a matter or transaction for a client
- to establish, exercise or defend a legal claim (including gathering evidence)

- complying with health and safety obligations
- to prevent fraud or other criminal offences
- to ensure network and information security, including preventing unauthorised access to our computer systems and electronic communications systems and preventing malicious software distribution

If you are a *matter data subject*, and are in a business, we may also use your contact details to pursue our legitimate interests for marketing our services (provided you have an opportunity to object and to unsubscribe).

In respect of our suppliers (or representatives of suppliers), we need to use your personal information primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate business interests of our own or those of our clients, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

- making a decision about your product, service or your general engagement
- determining the terms on which you will supply your goods or services to us or our clients
- paying you
- administering the contract we have entered into with you
- making decisions about your continued engagement
- making arrangements for the termination of your contract
- to progress a matter or transaction for a client
- to establish, exercise or defend a legal claim
- using contact details for marketing our services (provided you have an opportunity to object and unsubscribe).
- complying with health and safety obligations
- to prevent fraud or other criminal offences
- to ensure network and information security, including preventing unauthorised access to our computer systems and electronic communications systems and preventing malicious software distribution

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.

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
- where it is needed to assess your capacity on health grounds, subject to appropriate safeguards
- where it is needed in relation to legal claims or where it is needed to protect our clients' interests (or your interests) and you are not capable of giving or procuring consent, or where you 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 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
- 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

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 or your advisors for written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you or your advisors with full details of the information that we would like and the reason we need it, so that you or your advisors can carefully consider whether you or they wish to consent.

Information About Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so.

In the context for *matter data subjects*, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect our clients' interests (or your interests) and you are not capable of giving consent or where you 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 collect information about criminal convictions if it is appropriate and where we are legally able to do so. Where appropriate, we may be notified of such information directly by you or your advisors in the course of our client's matter or transaction.

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 authorised by law
- 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 will not be subject to decisions that will have a significant impact on you based solely on automated decision making, unless we have a lawful basis for doing so and we have notified you or your advisors.

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. Third party service providers of ours will only process

personal information on our instructions, and where they have agreed to treat the information confidentially and to keep it secure.

In respect of our own security obligations under the UK GDPR, we have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Othe than the disclosure of your personal information to our clients in respect of the matter or transaction, we limit access to personal information to those employees, agents, contractors and other third parties who have a business need to know and they will only process personal information on our instructions and they are subject to a duty of confidentiality.

PLEASE NOTE: this does not apply to personal information shared with our client in respect of the applicable matter or transaction connected to you, 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 the 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.

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 respect of *matter data subjects*, 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.
- We will need to retain client files, which may 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 on closure of the matter
- Basic details of Omny Law's clients must be available after closure for conflict checks in accordance with our regulatory obligations – they must adhere to the Solicitors Regulatory Authority's (SRA) Code of Conduct, the SRA being the relevant regulatory body under the Legal Services Act 2007.

Emails that may contain personal information of *matter data subjects* 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 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.

In respect of our suppliers (or representatives of suppliers), supplier contracts are periodically reviewed and our policy is to keep them for at least seven years after

termination which corresponds with the limitation period for contract claims under the Limitation Act 1980 plus one year (for appeals and possible technicalities). Emails that may contain your personal information are stored securely as previously stated in respect of *matter data subjects*.

Your Rights in Connection with Personal Information

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.

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).

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.

Object to processing of your personal information where we or our clients 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. For example, you always have the right to object where we are processing your personal information for direct marketing purposes.

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.

Request restriction of processing of your personal information. This enables you to ask us to suspend the processing of your personal information, for example to establish its accuracy or the reason for processing 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.

Request the transfer of your personal information to another party.

PLEASE NOTE: that this will not apply to the vast majority of matter data subjects because the right to a transfer (data portability as it is defined in the UK GDPR) only applies to personal information an individual has provided to a controller, where the processing is based on the individual's consent or the performance of a contract and when processing is carried out by automated means.

Withdraw consent. In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, 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 will no longer process the information for the purpose or purposes originally consented to, unless we have another legitimate basis for doing so in law.

If you wish to exercise any of the rights set out above, please contact us by email 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.

Please note that the personal information of representatives of businesses must be requested by the individual concerned (e.g. the board of directors cannot request the personal information of one of its employees, the employee should request this directly).

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.

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