

Recruitment Privacy Notice

Our commitment to your privacy	1
Adelphi Group of Companies – who are we?	1
About this privacy policy	1
Core Policy	1
How we use your information?	1
Personal data– what we hold and why we process it.....	2
Legal grounds for processing personal data	2
Where the personal data comes from	2
Who gets to see your personal data?	2
Internal use	2
External use.....	2
How long do we keep your personal data?	3
Transfers of personal data outside the UK and, or EEA.....	3
Right to be informed	4
Right of access to your information	4
Right of erasure (right to be forgotten)	4
Right of rectification	4
Opt-out of marketing communications	4
Withdraw your consent	4
Contact details	4
Complaints	5
Status of this notice	5
Changes to this privacy policy.....	5
ANNEX 1: Supplementary information	6
Glossary.....	6
Further information - Legal grounds for processing personal data	7
What are our legal grounds for processing?.....	7
Processing sensitive personal data	7
Personal data we process and our purposes	8

Recruitment Privacy Notice

This policy was last updated on the 31st of October 2023.

Our commitment to your privacy

Adelphi Group of Companies is committed to protecting and respecting your privacy. We take our responsibilities regarding the security of information that we have collected seriously. We are providing you with this Recruitment Privacy Policy because you are applying for work with us. It tells you how and why your personal data will be used and for how long we will usually retain it. Please read this policy carefully. If you have any questions, please contact compliance.team@adelphigroup.com.

Adelphi Group of Companies – who are we?

This privacy policy applies to the Adelphi Group of Companies. Adelphi Group is part of Omnicom Health Group, a division of Omnicom Group Inc. Find out more about the [Adelphi Group of Companies](#)

In this policy **ADELPHI**, **we**, and **us** means the Adelphi Group of Companies.

About this privacy policy

This privacy policy applies to **ADELPHI** who are processing personal data under Data Protection Legislation (see Glossary).

This Policy comprises the Core Policy and Annex 1 Supplementary information. The Core Policy contains key information, about the way **ADELPHI** use your personal data. Annex 1 -Supplementary information contains additional information.

Core Policy

How we use your information?

Like most businesses, we hold and process a wide range of information, some of which relates to individuals who are applying to work for us. This Recruitment Privacy Policy explains the type of information we process, why we are processing it and how that processing may affect you. It focuses on individuals who are applying to work for us and the data we process as part of that process. To find out more about our general privacy practices please consult the [Adelphi Privacy Policy](#).

We have a separate Workplace Privacy Policy that applies to our current and former employees. This Policy will be given to when you join the company and is also available to all members of staff on the **ADELPHI** intranet.

This Recruitment Privacy Policy explains:

- what personal data we hold and why we process it;
- the legal grounds that allow us to process your personal data;
- where the data comes from, who gets to see it and how long we keep it;
- how to access your personal data and other rights;
- how to contact us.

There is a Glossary on page 6, which explains what we mean by 'personal data', 'processing', 'special category personal data' and other terms used in this Recruitment Privacy Policy.

Personal data– what we hold and why we process it

We need to process and hold a range of information about the individuals who apply to work for us, including their personal details and work history.

We process this data for the purposes of our business, including management, administrative, employment and legal purposes. For more information see the section Personal data we process and our purposes on page 8.

Legal grounds for processing personal data

Under data protection legislation, there are various grounds on which we can rely when processing your personal data. In some contexts, more than one ground applies. Only certain lawful bases apply to **ADELPHI** during the recruitment process, and we have summarised these grounds as Contract, Legal Obligation, Legitimate Interests and Consent. For more information see the 'Glossary' on page 6 and 'Further information - Legal grounds for processing personal data' on page 7.

Where the personal data comes from

When you apply to work for us the initial personal data about you that we process is likely to come from you, or third-party recruiters, agents, and similar organisations. This data includes for example, contact details, employment history and information on your immigration status and whether you can lawfully work. The recruitment agency might ask you to complete a work preference questionnaire which is used to assess your suitability for the role you have applied for, the results of which are assessed by recruiters. Please read the recruitment agency's privacy policy for further information about the data that they collect and what it is used for.

We may also require references and information to carry out background checks. If you have concerns about this, you should speak to your recruiter or our HR department.

Who gets to see your personal data?

Internal use

Your personal data will be disclosed to managers, HR, Omnicom recruitment team and administrators for the purposes of considering your application as mentioned in this document. If you are applying for a general position within **ADELPHI** (for example, an Adelphi graduate position) then your details may be passed to relevant Adelphi companies. If you are applying for a specific role with an Adelphi company your details may be passed to another Adelphi company, if we feel there may be a suitable position.

External use

We will only disclose your personal data outside **ADELPHI** if disclosure is consistent with one or more of our legal grounds for processing and if doing so is lawful and fair to you.

We may disclose your personal data if it is necessary for our legitimate interests as an organisation or the interests of a third party, such as if we use a recruitment portal managed by a third-party provider, we may send your personal data on to that third party (but we will not do this if these interests are over-riden by your interests and rights in particular to privacy).

We may also disclose your personal data outside **ADELPHI**:

- if you consent to the disclosure;
- where we are required to do so by law;
- in connection with criminal or regulatory investigations.

Specific circumstances in which your personal data may be disclosed include:

- Disclosure to organisations that process data on our behalf such as: our payroll service; insurers and other benefit providers; our bank; organisations that host our IT systems and data; professional service providers such as legal advice. This would normally occur if you accepted an offer from us and would be carried out as part of the on-boarding process;
- To third party recruitment consultants and similar businesses (including online recruitment portals) as a part of the recruitment process.

How long do we keep your personal data?

We will retain your personal information for a period of 12 months after we have communicated to you our decision about whether to appoint you. We retain your personal information for that period so that we can:

- Show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way.
- Let you know about any further opportunities, that may arise in the future, that we think may be of interest to you based on your personal information and that we may wish to consider you for.

After this period, we will securely destroy your personal information in accordance with applicable laws and regulations. We may retain CV's for longer than 12 months if you have explicitly asked us to do so, or we have your explicit consent.

If you become employed by us, we will keep your personal data for the duration of your employment and for a fixed period afterwards. Our Data Retention and Deletion Policy contains details of the retention period of employment records.

If your data is only required for a short period of time (e.g., CCTV footage data) this will be deleted on a rolling basis.

Transfers of personal data outside the UK and, or EEA

ADELPHI are a global organisation and to manage recruitment applications, we may transfer your personal data outside of the UK or EEA to members of our group and processors in the United States.

Where we need to transfer your information outside of the UK or EEA, we do so to countries which have been determined by the UK Government or European Commission to have an adequate level of data protection or by using a variety of legal mechanisms, including Intra company data sharing agreements and Model Clauses, to help ensure your rights and protections.

Occasionally we will transfer personal data to other jurisdictions in which we are established. Some of our systems are hosted in the United States, we will ensure that the transfer is lawful and that there are appropriate security arrangements.

Your data protection rights

You have specific rights in relation to your personal information provided to **ADELPHI**, although in some cases these rights are subject to certain conditions and limitations. To exercise any of these rights please reach out to us using the contact details in the section Contact details on page 4.

Right to be informed

You have the right to be told how your personal information is/will be used. Our Privacy Policy and our Recruitment and Workplace Privacy notices are intended to provide a clear and transparent description of how your personal data may be used. We will also inform you if your personal data has been involved in a personal data breach which may cause you distress or harm.

Right of access to your information

You can request a copy of the personal information which we hold, and which relates directly to you. You can contact us in writing or by phone using the contact details in this section. Please ensure that you include your name and clear instructions on what information you need. You do not need to state the reason for your request. We will provide this information free of charge and we will provide this information to you as swiftly as possible and within one month of your request unless the request is complex or is numerous requests. If this is the case, we will inform you within one month of your request about the reason for the extension of time.

It should be noted that if your request is excessive, disproportionate, or repetitive we may ask you to narrow the focus of your request, or we are permitted to decline the request.

Right of erasure (right to be forgotten)

You have the right to have your personally identifiable data deleted. This is only applicable to information for which we have no lawful basis for retention.

Right of rectification

If you believe the records that **ADELPHI** keep are inaccurate or incomplete, you have the right to ask for these to be corrected or enhanced.

Opt-out of marketing communications

You have an absolute right to opt-out of hard copy or electronic marketing communications that we send to you at any time. You can exercise this right by clicking on the “unsubscribe” or “opt-out” link in the marketing e-mails we send you, alternatively you can request to unsubscribe by sending an email. You can also opt-out of other forms of marketing (such as postal marketing or telemarketing), by contacting us using the contact details below.

Withdraw your consent

If we have collected and processed your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Contact details

Adelphi Group (UK office), ATTN: DPO/Compliance Department

Adelphi Mill, Bollington

Cheshire SK10 5JB, UK

Email: compliance.team@adelphigroup.com

Adelphi Group (Netherlands office), ATTN: DPO/Compliance Department

Professor W.H. Keesomlaan 4,
1183 DJ Amstelveen, The Netherlands
Email: compliance.team@adelphigroup.com

Adelphi Group (US office), ATTN: DPO/Compliance Department

2005 South Easton Road, Suite 300, Doylestown, PA 18901
Email: compliance.team@adelphigroup.com

Complaints

If you have complaints relating to our processing of your personal data, in the first instance you should raise these with the **ADELPHI** compliance department; see section Contact details. If you remain unhappy you can raise a complaint directly with the relevant supervisory authority.

In the UK: Information Commissioner's Office (ICO). They can be contacted via their website <https://ico.org.uk/>

In the Netherlands: Autoriteit Persoonsgegevens. They can be contacted via their website <https://autoriteitpersoonsgegevens.nl>

Status of this notice

This Recruitment Privacy Policy does not form part of any contract of employment you might enter into and does not create contractual rights or obligations. It may be amended by us at any time.

Changes to this privacy policy

We keep our privacy policy under regular review and reserve the right to revise it at any time. There is a date at the beginning of this policy which indicates the date it was updated. Please revisit this policy each time you consider giving personal information.

ANNEX 1: Supplementary information

Glossary

'Data Protection Legislation' means all applicable legislation, local laws and regulations relating to data protection and privacy, including the EU General Data Protection Regulation (EU GDPR) and the UK General Data Protection Regulation (UK GDPR), together with any national implementing laws in the UK, any Member State of the European Union or, to the extent applicable, in any other country, each of the foregoing as amended, repealed, consolidated, or replaced from time to time.

'Personal data' is information directly relating to you, or from which you may be indirectly identified. It must be processed by electronic or automatic means, or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you.

Personal data **'processed automatically'** includes information held on, or relating to use of, a computer, laptop, mobile phone, or similar device. It covers data derived from equipment such as access passes within a building, data on use of vehicles and sound and image data such as CCTV or photographs.

'Processing' means doing anything with the data. For example, it includes collecting it, holding it, disclosing it, and deleting it.

'Special Category personal data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, physical or mental health, sexual orientation, sex life, trade union membership and genetic and biometric data. These types of data are subject to special protection under the law. In the UK this also includes actual and alleged criminal convictions.

References in the Recruitment Privacy Policy to **'employment'**, **'work'** and similar expressions include any arrangement under which an individual works for us or provides services to us or applies to provide services. This includes individuals who are our employees and also those who provide services under a freelance or independent contractor arrangement. Similarly, when we mention an **'employment contract'**, this should be taken to include any contract with an employee, a freelancer, or a contractor; and when we refer to ending your potential **'employment'**, that includes terminating a freelance engagement or a contract for services.

We use the word **'you'** to refer to anyone within the scope of this Recruitment Privacy Policy.

Further information - Legal grounds for processing personal data

What are our legal grounds for processing?

Under data protection legislation, there are various grounds on which we can rely when processing your personal data. In some contexts, more than one ground applies. We have summarised these grounds as Contract, Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

Term	Ground for processing	Explanation
Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract.	This covers carrying out our contractual duties and exercising our contractual rights.
Legal obligation	Processing necessary to comply with our legal obligations.	Ensuring we perform our legal, fiduciary, and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination.
Legitimate interests	Processing necessary for our or a third party's legitimate interests.	We (and third parties) have legitimate interests in carrying on, managing, and administering our respective businesses. Part of managing businesses will involve the processing of your personal data. Your data will not be processed if, in processing your data, your interests, rights and fundamental freedoms related to the data override our businesses' interests in processing the data for businesses purposes.
Consent	You have given freely given, specific, informed, and affirmative consent to processing your data.	In general processing of your data in connection with employment is not conditional on your consent. But there may be occasions where we do specific things such as provide a reference and rely on your consent to do so.

Processing sensitive personal data

If we process special category personal data about you (for example (but without limitation), processing your health records to assist us in ensuring that we provide you with reasonable adjustments during any recruitment process), as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that an additional ground for processing special category personal data applies. In outline, these include:

- Processing being necessary to comply with employment law, in so far as it is authorised by law

or collective agreement;

- Processing relating to data about you that you have made it manifestly public (e.g., if you have told us, you are ill);
- Processing being necessary for the purpose of establishing, making, or defending legal claims;
- Processing being necessary to provide any necessary reasonable adjustments during the recruitment process.

Personal data we process and our purposes

The purposes for which we process your personal data, examples of the personal data that may be processed and the grounds on which we process it are set out in the table below.

The examples in the table cannot, of course, be exhaustive. For example, although the table does not mention personal data relating to criminal offences, if we were to find out that someone applying to work for us was suspected of committing a criminal offence, we might process that information if relevant for our purposes.

Purpose	Examples of personal data that may be processed	Grounds for processing	Retention
Recruitment	Standard data related to your identity (e.g. your name, address, email address, ID information and documents, telephone numbers, place of birth, nationality, contact details, professional experience and education (including university degrees, academic records, professional licenses, memberships and certifications, awards and achievements, and current and previous employment details), financial information (including current salary information) language skills, and any other personal data that you present us with as part of your application related to the fulfilment of the role. Information concerning your application and our assessment of it, your references, any checks we may make to verify information provided and any information connected with your right to work. If required for the role we may perform background checks with your consent. If appropriate we may also perform a criminal record search. Within the EU and the UK, we will only perform this if we are legally required to do so or have your explicit consent. If necessary, we will also process special category information concerning your health, any disability in connection with any adjustments to working arrangements. Please note also that we may process your personal data both in relation to an application for one job, and in relation to an application for another job for which we feel you may be suitable.	Contract Legal obligation Legitimate interests Consent	Duration of employment and for 6 years after employment ceases.

Administering our recruitment process	Evaluating your experience and qualifications against the requirements of the position you are applying for. Administering our online careers portal. Communicating with you in respect of any offer of employment we choose to make and providing you with information about our onboarding process	Contract Legal obligation Legitimate interests	Unsuccessful candidates: deleted after 12 months. unless extended by consent. Successful candidates – CV kept on record for duration of employment.
Entering into a contract with you (if you are made an offer by us)	Information on your terms of employment from time to time including your hours and working patterns, your pay, and benefits, such as your participation in pension arrangements, life, and medical insurance; and any bonus or share schemes	Contract Legal obligation	For duration of employment and for 6 years after employment ceases.
Contacting others on your behalf	For the purpose of gathering references.	Contract Legitimate interests	6 years.
Financial planning and budgeting	Information such as your proposed salary and (if applicable) envisaged bonus levels.	Legitimate interests	For duration of employment and for 6 years after employment ceases.
Payroll administration	Information on your bank account, pension contributions and on tax and national insurance. Your national insurance number or other government issued identifier.	Contract Legal obligation	For duration of employment and for 7 years after employment ceases.
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability, and age as part of diversity monitoring initiatives. Such data will be aggregated and used for equality of opportunity monitoring purposes. We may share aggregated and anonymized diversity statistics with regulators if formally required / requested.	Consent Legal obligation	7 years.
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation	7 years.

Please note that if you accept an offer from us the business will process further information as part of the employment relationship. We have a separate Workplace Privacy Policy that applies to our current and former employees. This notice will be given to when you join the company and is also available to all members of staff on the **ADELPHI** intranet.