

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

Introduction

This Policy sets out the obligations of AMD regarding data protection and the rights of clients, subcontractors, suppliers and business contacts (“data subjects”) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company’s responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

All employees, agents, contractors, or other parties working on behalf of the Company handling

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

personal data will be appropriately supervised;

All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

Where any agent, contractor or other party working on behalf of the Company handling data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Purpose of Policy

AMD is committed to maintaining the highest standards of compliance with data protection requirements in line with the Data Protection Act (DPA) 2018 and legislative amendments.

This privacy notice and policy tells you what to expect when AMD collects personal information. It applies to information we collect about visitors to our website, job applicants, current and former employees.

We process employee's data in order to fulfil our contractual obligations to our employees and to comply with our common law and statutory obligations. In respect of our vehicle tracking system we process personal data for the company's legitimate interest.

We hold and process data in order to:

- Administer and maintain personnel records;
- Pay and review salary and other remuneration benefits;
- Provide and administer benefits (including if relevant, pension, life insurance, permanent health insurance and medical insurance);
- Undertake performance appraisals and reviews;
- Maintain sickness and other absence records;
- Take decisions regarding fitness for work;
- Provide references and information to future employers;
- Provide information to governmental and quasi-governmental bodies for tax, National Insurance, social security and other purposes;
- Provide information to future purchasers of the company and to prospective transferees of any part of the business.

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

Employer's Obligations

AMD complies with all appropriate data protection principles. We will therefore:

- Process data lawfully, fairly and in a transparent manner and process it only for specified and lawful purposes;
- Ensure that all data obtained is adequate and relevant to those lawful purposes and is accurate, up to date and kept no longer than necessary;
- Process all data in accordance with each employee's statutory rights;
- Take the appropriate security measures to protect the data from unauthorised disclosures.

Collection and Management of Employee Data

Staff who process employees' personal data have a duty to ensure that information is only collected for its stated purpose, that it is factual and that information is kept securely and destroyed in accordance with company and statutory regulations.

All members of staff who have access to other staff members' personal data as part of their job must at all times ensure that:

- Information is used only for the purpose(s) for which it was collected
- Data confidentiality is maintained at all times
- Data accuracy is maintained
- Data is held securely
- Only data necessary for the conduct of normal company business is retained
- Confidential data, whether held in paper format or electronically, is destroyed when no longer required.

Disclosure of Employees' Personal Data

Employees' information should not be disclosed to anyone without proper authority. Staff should contact the PA to the Directors, if they have any questions regarding disclosure of personal data. Any employee who discloses another individual's personal data without proper authorisation may be subject to disciplinary proceedings.

Internal Disclosure

Personal information should only be disclosed to other members of AMD's staff if the staff member concerned has given permission or if the disclosure is necessary for the legitimate interests of the company. Personal information must not be disclosed merely for social reasons.

External Disclosure

Generally, personal data should not be given out externally, except where there is a legal or contractual requirement to do so, without the permission of the staff member concerned. It is

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

permissible to provide personal data in **emergency** situations, (i.e. where the individual's or someone else's life may be in danger).

Personal data should not be disclosed over the telephone unless you are certain of the identity of the caller and that you are authorised to release the information.

Requests for information from the police or other investigatory bodies should be directed to the PA to the Directors.

Reporting a Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Examples can include:

- Access by an unauthorised third party
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

If you become aware of a personal data breach, you must report this to PA to the Directors, without delay.

Should there be a privacy related breach / incident, the Operations Directors will advise the affected clients within 24 hours, if there is the potential that the breach could impact them.

Employee's Rights

Under current Data Protection law, you have rights as an individual that you can exercise in relation to the information we hold about you. Where these relate to current or former employees, your rights are set out in our separate Data Protection policy which is included in the Employee Handbook.

Access to personal information

Individuals can find out if AMD Environmental holds any personal information by making a 'subject access request'. If we do hold information about you we will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

This information will be provided within one month of receiving such a request. To make a request to AMD for any personal information we may hold, you need to put the request in writing addressed to the PA to the Directors at the address provided below.

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need over the telephone.

If, on viewing that personal data processed by ourselves, an employee considers the data to be inaccurate, then he or she has the right to ask AMD to amend any inaccuracies or to remove any data that is inaccurate or out of date. The employee also has the right to request that the company restricts or stops processing the data. Please note that this does not apply where we are processing data in fulfilment of our legal obligations. Any such request should be made to the PA to the Directors in writing.

AMD has a requirement to maintain accurate and up to date information, and for that purpose there is an obligation upon employees to keep up informed of all changes to personal data including changes of address, marital status and next of kin from time to time.

Visitors to our website

When someone visits <http://www.amdenvironmental.co.uk> we use a third party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is processed in a way that does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those using our website.

A separate Privacy Notice relates to use of our website, including Cookies Policy. Here is a link to this policy:

<http://www.amdenvironmental.co.uk/privacy-policy/>

Search Engine

Our website and decision notice search is powered by Wordpress. No user-specific information is collected, the system simply searches the content of the website when someone puts in a search item.

Security and performance

AMD uses a third party service, Aptus Technology to help maintain the security and performance of our company server and the integrity of our organisation. Aptus Technology maintains rigorous security policies and practices across the company. A copy of this company's Security Policy can be found here:

<http://aptustechnology.co.uk/it-security-policy/>

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

Recruitment Process

What will we do with the information you provide to us?

All the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

What information do we ask for, and why?

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You do not have to provide what we ask for, but it might affect your application if you don't.

Application stage

We ask you for your personal details including name and contact details. We will also ask you about your

previous experience, education, referees and for answers to questions relevant to the role you have applied for. Our recruitment team will have access to all this information.

You may also be asked to provide equal opportunities information. This is not mandatory information – if you do not provide it, it will not affect your application. This information will not be made available to any staff outside our recruitment team, including hiring managers, in a way that can identify you. Any information you do provide will be used only to produce and monitor equal opportunities statistics.

Assessments

We may ask you to participate in assessment days; complete tests or occupational personality profile questionnaires; and/or to attend an interview – or a combination of these. Information will be generated by you and by the company. For example, you might complete a written test or we might take interview notes. This information is held by AMD.

Retention of information following interview and assessment

If you are unsuccessful following interview or assessment for the position you have applied for, we may ask if you would like your details to be retained in our talent pool for a period of 12 months. If

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

you say yes, we would proactively contact you should any further suitable vacancies arise. If you do not wish us to keep your information for this reason, it will be deleted 6 months after the interview or assessment.

Conditional offer

If we make a conditional offer of employment, we will ask you for information so that we can carry out pre-employment checks. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity, and reliability.

You will therefore be required to provide:

- Proof of your identity – you will be asked to attend our office with original documents, we will take copies.
- Proof of your qualifications – you will be asked to attend our office with original documents, we will take copies.
- We will contact your referees to obtain references, using the details you provide in your application.
- We will also ask you to complete a questionnaire about your health. This is to establish your fitness to work.

Disclosure & Barring Service Checks

For certain jobs we may need to submit your details to the DBS Service which processes requests for criminal records check. AMD is a registered employer with the Service and entitled by law to ask you to reveal your full criminal history (other than protected cautions and convictions), including spent convictions - also known as asking 'an exempted question'.

An exempted question applies when the individual will be working in specific occupations, for certain licenses and specified positions. These are covered by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975.

Here is a link to the DBS Code of Practice, with which AMD is fully compliant.

<https://www.gov.uk/government/publications/dbs-code-of-practice>

We use three specialist companies, for our DBS and other security checks. These are Complete Background Screening, Experian and GBG Know Your People. Here are links to these companies' privacy policies:

<https://www.cbsscreening.co.uk/privacy-policy/>

<https://www.gbgplc.com/privacy-policy> which explains how GBG processes data for the purposes of obtaining a Disclosure from DBS

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

<https://www.experian.co.uk/consumer/dsar/privacy.html> This explains what information Experian collect and who they share it with. The agreement between AMD Environmental and Experian specifies that Experian will only collect the information that is absolutely necessary to carry out the security screening.

Enhanced Security Clearance

Some roles require a higher level of security clearance. This will be clear in the job advert. Or you may be transferred to a role requiring higher security clearance if you change jobs within the company. If this is the case, then you will be given details of the organisation in question, together with their privacy policy, in advance of your details being passed to that organisation for security clearance.

For contracts involving companies or sole traders, we carry out checks through a specialist firm, Credit Safe.

That company's Privacy statement and DPA statement are here:

<https://www.creditsafe.com/us/en/product/privacy/privacy-policy.html>

<https://www.creditsafe.com/gb/en/more/about/gdpr.html>

Attendance at Client Premises

As a pre-condition of admittance to some client premises we are required to submit your name and proof of certain qualifications/copy of CSCS card and other proof of identity, for example a copy of your passport or driving licence. This information will be held securely and will not be shared with any third party without your consent.

Use of data processors

Data processors are third parties who provide elements of our recruitment service for us. We have contracts in place with our data processors. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

Offers of Employment

If we make a final offer, we will also ask you for the following:

- Bank details – to process salary payments
- Emergency contact details – so we know who to contact in case of an emergency at work

	Data Protection Policy	Ref:	AMD010
		Issue:	1.0
		Date:	01.12.2023
		Review:	30.11.2024

Personnel Records

If you accept a final offer from us, your personal data will be held on file on our company server. This is held in a secure, access restricted location and kept up to date with the relevant software updates and anti-virus protection. Your personal data will never be published or distributed by us without your prior permission.

Payroll

If you are employed by AMD Environmental, relevant details about you will be provided to our company accountants, Peachey & Co. who administer payroll services. This will include your name, bank details, address, date of birth, National Insurance number and salary. Here is a link to the company's website, which holds copies of their security and privacy statements :

www.peachey-accountants.co.uk

The People's Pension/ B&CE

B&CE are the administrators of AMD Auto Enrolment Pension Scheme, The People's Pension. You will be auto-enrolled into the pension scheme.

Third Parties

This policy is included within all of our contracts and purchase orders issued by AMD. AMD supply chain are bound by the contents of this policy, and must ensure that their employees and supply chain adhere to this policy at a minimum.

SIGNED:



Mr Jon King
Managing Director
01.12.2023



Mr Marcus Sullivan
Managing Director
01.12.2023