A|M|S

AMS Data Protection Policy

Version 9 May 2026

A|M|S

Table of Contents

A|M|S

POLICY STATEMENT

Everyone has rights regarding how their personal data is obtained, stored, managed, processed, transferred, retained, and destroyed. During our activities we will collect, record, store and process personal data about our staff, clients, candidates, suppliers and other third parties. We recognise the need to treat it in an appropriate and lawful manner.

We update this policy annually to reflect changes in law and regulatory guidance. Until the legislation has been published and is legally binding, we do not make such changes. We are monitoring any proposed legislation. Please contact any member of the Privacy Office or your regional legal support team to assist you if you have any queries about impending law.

Affiliates, Subsidiaries and “Non-Employee Staff”

This policy applies to the directors of Alexander Mann Group Limited (Directors’), its officers, employees, and ‘non-employee AMS staff (individuals performing services to or on behalf of AMS, including temporary workers, and consultants). For clarity, where used in this document, the terms ‘AMS’, ‘AMS Group’, ‘the Group’, ‘we’, ‘us’ or ‘our’ refer to affiliates or subsidiaries of Alexander Mann Group Limited that link to or reference this policy. In addition, this policy applies to the directors of the group’s holding companies up to and including Auxey Holdco Limited.

Independent Contractors

To protect the vital interests of AMS and its clients, contractors shall comply with the procedures, standards and guidelines set in this policy to the extent that they are reasonably applicable to them as independent contractors in the provision of services to AMS and/or its clients. This requirement is not to replace any contractual obligation in relation to AMS’s and/or its clients’ policies, procedures, standards, and guidelines that contractors are bound by and is not intended to create or imply any supervision, direction, control, mutuality of obligation or employment relationship between the parties.

ABOUT THIS POLICY

The types of information that we may be required to manage include personal data of candidates, clients, employees, supporters, recruiters and suppliers of AMS and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in data protection legislation

worldwide due to the nature and reach of our global operations. To accommodate the variations in this legislation we have adopted a set of standards that can be applied using the individual rules of the UK/EU GDPR (General Data Protection Regulation), PIPL for China, DPDPA for India and the Data Privacy Act in the Philippines as our guide.

This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to 'processing' which by definition under the EU GDPR means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This policy should be adopted alongside the AMS Data Retention Policy and AMS Information Security Policy and AMS AI Policy which together form the suite of AMS policies safeguarding the way we work with personal data.

The Data Protection Officer is responsible for ensuring compliance with global data protection legislation and with this policy. The Data Protection Officer can be contacted at dataprotection@weareams.com

If you consider that the policy has not been followed with respect to personal data about yourself or others, you should raise the matter with your line manager and the Data Protection Officer. If you prefer you may also raise this through AMS Raise Your Concern

DO THE DATA PROTECTION RULES APPLY?

It is important to understand how easy it is to fall within data protection rules in your country and the countries where you work. Are you handling personal data either in paper form or electronically on a computer, tablet, or smart phone? Yes. Then, you are most likely to have to comply with data protection rules.

WHAT ARE THE DATA PROTECTION RULES AND HOW DO I COMPLY WITH THEM?

Looking at the data protection rules from a basic and general position, the rules require data controllers/owners to ensure they are fair, transparent, and lawful in the way they manage someone else's personal data. The rules require the data user to explain what they will do with it and not do anything else. They require the data controller to make sure the person who owns the personal data is aware of their rights, has a point of contact and understands what will happen with their personal data when they share it with the data controller. In most

countries around the world the best way for a data controller to show they have fulfilled their obligations is to either inform the person via a privacy notice or to obtain a person's consent to share their personal data with them, for the reasons and purposes stated.

At AMS we apply a risk-based approach to data protection. The level of documentation, assessment and oversight required for any processing activity will depend on the nature, scope, context and purposes of the processing, and the level of risk posed to individuals' rights and freedoms. Higher-risk processing will be subject to enhanced measures, while lower-risk processing may be addressed through proportionate controls and standard documentation.

Each step in understanding the typical application of most countries' data protection rules is set out below. This is a general overview, and each country has a more precise definition of each step which the Data Protection Officer can provide if you believe you need it.

WHAT IS PERSONAL DATA

The first step in understanding whether data protection rules apply to what you are doing is whether the information you are working with is personal data as defined by the data protection rules.

Personal data is information relating to an individual irrespective of age, from which that individual can be identified. This can include name, email address, correspondence address, mobile telephone number, social security numbers, IP addresses. It can also include combinations of personal data that enable identification of an individual, for example, job title, gender and employer, or information AMS already holds on an individual combined with information provided by that individual.

Pseudonymisation means processing personal data so that it cannot be attributed to an individual without the use of additional information. Pseudonymised data remains personal data where re-identification is possible and is therefore processed in accordance with applicable data protection laws. By contrast, fully anonymised data, where individuals are no longer identifiable by any reasonably likely means, falls outside the scope of data protection law.

Most countries include an additional personal data definition covering "sensitive personal data" or "special categories of data." This includes information about an individual's racial or ethnic background, political opinions, religious or philosophical beliefs, trade union

membership, genetic data, biometric data, health information, credit history, and criminal record. This information is more carefully protected and specific consent to processing personal sensitive information may be necessary.

PROCESSING PERSONAL DATA

If you are working with personal data, it is important to understand what you are doing with it and whether this forms part of the data protection rules.

When processing personal data, AMS must ensure it is handled lawfully, fairly and transparently in line with this policy and applicable data protection laws. All processing must be assessed for compliance, with the level of assessment and documentation applied proportionately based on risk. Higher-risk processing may require enhanced oversight.

Processing personal data is governed by data protection rules. It has a broad definition and includes (but is not limited to) the following:

Obtaining	Handling	Organising	Consulting	Transfer
Recording	Holding	Adapting	Use	Disposal
Retrieval	Storing	Altering	Disclosure	Destruction

Manual, automated and AI-assisted processing are governed by this policy and the data protection rules.

A.I ASSISTED DATA PROCESSING

AI-assisted processing is a form of processing and must be assessed in accordance with this policy, the AMS Artificial Intelligence (AI) Policy and applicable data protection laws. Where AI is used to support or make decisions that may significantly affect individuals, additional assessment, controls and transparency requirements may apply. Examples of AI tools (which may involve AI-assisted processing of personal data) include Generative AI assistants (e.g., Microsoft Copilot or similar tools) used to draft, summarise or analyse content that contains personal data. Large language model (LLM) chat tools (e.g., ChatGPT or similar tools) used to classify or extract information from text that contains personal data. Automated transcription tools used to convert audio or video recordings (e.g., calls or meetings) into text that may contain personal data. AI-enabled recruitment tools used for CV parsing, candidate matching, screening, ranking or shortlisting (where these activities involve personal data). AI-enabled monitoring, security or fraud/anomaly detection tools that analyse user activity, communications or system logs where these identify or relate to individuals.

Human oversight and escalation: Where AI-assisted or automated processing is used in connection with personal data, appropriate human oversight must be in place, including the ability to review outputs and intervene where necessary. Where processing could significantly affect an individual, AMS will ensure there is a clear route for escalation to an appropriate decision-maker and, where required by applicable law, individuals will be informed of their right to request human intervention and to contest a decision. Any suspected personal data incident involving AI tools must be reported in accordance with the AMS Incident Management Process. Concerns about non-compliance with this policy may be raised with the Data Protection Officer, your line manager, or via AMS Raise Your Concern

With such a broad definition, most of our day-to-day activities fall within the data protection rules and we must make sure that any personal data we process complies with them.

CAN I PROCESS PERSONAL DATA

The good news is yes, you can, but only if you comply with some additional obligations. These are:

1. Providing the individual with fair processing information; and
2. Ensuring that any processing complies with the standard conditions for processing.

FAIR PROCESSING INFORMATION

The easiest way to understand what "providing fair processing information" means is to ask yourself what information you would like to know before giving your personal data to a third party. Fair processing information is really another way of describing the provision of a data protection statement or privacy notice or notice of fair processing. This information must be provided BEFORE any personal data is processed and it helps the individual decide whether they wish to provide their personal data or not. Without this information how can anyone decide whether to share their personal data with an organisation?

Fair Processing Information must include the following:

1. The identity of the data controller or its representative.

The data controller is the person or organisation that decides the purpose for which the personal data is being processed, and the means for how it is processed. Importantly, it is the individual or organisation that is accountable under most countries' data protection rules. For example, when we are providing permanent recruitment services for a client, the

client is the data controller, however, when we are recruiting for AMS, AMS is the data controller. Equally, when we are asking for information from our employees, AMS is the data controller, when we provide consultancy services to a client, AMS is the data controller. Whether we are the data controller or not, complying with the data protection rules in the countries we are operating in is vital to our successful delivery solution and reputation.

We use data controllers in this policy because in some countries the law distinguishes between those that control the data and those that simply process it on their behalf. However, some countries where we operate do not distinguish between the two and anyone processing personal data must do so in accordance with the law. In these countries, even if we are processing data on behalf of our client, AMS is as accountable to the data subjects as the client.

2. The purpose for which the personal data is being processed.

Why is personal data being obtained, stored, retrieved, shared, or used? To decide whether to share it, an individual must understand what their personal data will be used for and who it will be shared with.

3. Further information that it is fair to disclose.

What does this mean? It varies from country to country but to provide a global answer the following must always be included:

- The identity of the people who will receive the information, and if there is an international data transfer – this may be simply the people or organisation requesting it, but it is more likely to include any other companies they work with to process the personal data, for example AMS as a provider of recruitment outsourcing services, the software company that stores and processes the personal data.
- The lawful basis on which the data is processed, for example under the GDPR there are six lawful basis which allow for personal data to be processed. It is especially important to ensure that the lawful basis being applied is acceptable for this purpose. Ask the Privacy Office for support in determining this for the purpose of the privacy statement. If the organisation believes that it has a legitimate interest, it must complete an assessment that describes the legitimate interest that it has in the privacy statement or fair processing notice.
- The consequences of not providing the personal data. How can fair processing information be fair if it does not provide details of what will happen if the information is not provided or not provided accurately? In the case of

recruitment, not providing personal data is most likely to result in the individual not being put forward for a role.
- Whether sensitive or special categories data is being processed.
- The right of the individual to access and rectify incorrect personal data, to withdraw their consent to processing, to object to specific types of processing, for example marketing, to erase personal data, and the right to data portability.
- In the EU, individuals have the right to lodge a complaint with the authorities, and this must also be included in the privacy statement or fair processing notice.
- Information about the transfer of personal data – will this take place, and if so, what security measures are in place to protect the personal data. Further details on data information transfer rules are set out in section 12.
- Information about retention of personal data. For further information on AMS's position on this please see the AMS Data Retention Policy.
- Some countries consider that for the fair processing information to be provided "fairly" it must be given in a language that the individual understands. This can be interpreted as the individual's native language. AMS's position is that unless explicitly required by local law, the fair processing information must be in the language that the individual is expected to speak for business purposes.
- GDPR also requires information about where personal data is used to build a profile of an individual to predict behaviour, and where automated decision making is made that may impact on the person. This will include automated decisions taken within a sourcing and selection process.

Certain countries require additional information to be provided, and you may seek advice on this from the Data Protection Officer.

STANDARD CONDITIONS FOR PROCESSING

The last step needed before any personal data can be processed is for the standard conditions for processing to be met. These are:

1. Have you given the person fair processing notification via a Privacy Notice or a Data Protection Statement?

The contents of the fair processing notification vary from country to country, however in general it should contain the information contained in the above section.

2. Do you have individual consent?

Some countries require explicit written consent; other countries consider consent to have been given by virtue of the fair processing information being posted on an organisation's

website. Where consent is obtained from a person, usually electronically, it should be recorded so that it can be evidenced if questioned in the future.

Depending on the country, consent from minors may require consent from the child's guardian. In deciding whether this additional consent is necessary we consider the age of the child and their ability to understand the implications of sharing their personal data. In some countries, actual age limits are provided where guardian consent is required. AMS very rarely deals with personal data of a minor, however if you believe you will be, please contact the Data Protection Officer for specific advice.

Consent is not needed in certain prescribed circumstances including where an individual's personal data must be disclosed as required by law or in response to a request from law enforcement agencies.

3. The personal data must be.

    - Processed fairly and lawfully, and transparently – if the information listed above under the Fair Processing Information heading is provided in a fair processing notice, then the fair and lawful, and transparent requirement will be satisfied.
    - Collected for specific, explicit, and legitimate purposes and not processed in a manner incompatible with those purposes. Purpose is important and using personal data for a purpose that was not disclosed to the individual is a deception. If an additional purpose is required to the one for which the person was informed in the Fair Processing Notice, further notification must be provided, or consent must be obtained from the individual.
    - Adequate, relevant, and not excessive. Do not collect any more personal data than is needed for the purpose.
    - Accurate and where necessary up to date. Our standard privacy notices highlight that personal data must be kept up to date. In relation to employee information, AMS employees are urged to maintain their personal data up to date.
    - Kept in an identifiable form in line with AMS Data Retention Policy . The AMS Data Retention Policy sets out more details on this point and includes a list of time periods for which certain types of personal data must be retained. It also sets out the data review process which must be undertaken prior to personal data destruction.
    - Secure. It is vital that information is kept secure, and in line with AMS Information Security Policy.

A|M|S

LAWFUL AND LEGITIMATE PROCESSING OF PERSONAL DATA

If all the conditions listed above are fulfilled then generally, you will be processing personal data lawfully and legitimately. However, if you are concerned about the application of a specific country's rules then please contact the Data Protection Officer for more specific guidance.

SECURITY

The security of personal data provided by us or to us in accordance with the data protection rules is as important as complying with the rules themselves. The AMS Information Security Policy sets out further guidance and should be read alongside this policy. Together, the two form our minimum security and information requirements for all personal data.

TRANSFER OF PERSONAL DATA

The transfer of personal data is also governed by data protection rules. A transfer can take place when personal data is stored and processed by software that hosts the data in a different country from the country where it was collected. A transfer can also take place when personal data is shared within AMS by offices in different countries, for example data sourced in the UK for recruitment in the US.

The data protection rules relating to transfer of personal data generally state that personal data may only be transferred to a different country if that country has in place or agrees to put in place procedures that are known to provide protection for personal data equal to those procedures in place in the country where the personal data is being transferred from. For specific information regarding the GDPR and the EU please review the following section.

TRANSFERS OF PERSONAL DATA AND THE EEA

There are no restrictions of personal data transfer within the EEA (EU plus EEA countries of Iceland, Norway, and Liechtenstein). This is because the EEA countries have all implemented EU law (the GDPR) in their national data protection rules.

For transfers of personal data originating in the EEA, there are a few options:

The European Commission has issued a decision on other countries that are deemed to have equivalent national protection rules in place which allow for free movement of data. At the time of writing these are: -

Andorra	**Canada	Guernsey	Israel	Switzerland
Argentina	Faroe Islands	Isle of Man	Jersey	New Zealand
Uruguay	Japan***	*United Kingdom	Republic of Korea	Brazil

For transfers to all other countries, Standard Contract Clauses (Model Clause) Agreements must be put in place to ensure that there is "adequacy" of protection in place before the transfer takes place.

*Under the GDPR and the LED

**Commercial Organisations

***Private Sector

TRANSFERS FROM THIRD COUNTRIES

Transfers from (i) non-EEA countries into the EEA and (ii) non-EEA countries into another non-EEA country are governed by the data protection rules of the country where the data is being transferred from. Each country varies and therefore you should always check with the Data Protection Officer

RIGHTS OF INDIVIDUALS

Most data protection rules provide for individuals to have a right to request to see the personal data that an organisation is holding, retaining, processing about them. This request is referred to as an Individual Rights Request or Subject Access Request. Any member of staff who receives a written request should forward it to the Privacy Office at dataprotection@weareams.com immediately as there is a time limit of 30 days within which we must provide a response.

While fees may be charged in some countries, from May 26th, 2018, a fee can no longer be charged for EU data subjects. The same process should be followed, which is to inform the Privacy Office and Data Protection Officer immediately.

PROVIDING INFORMATION TO THIRD PARTIES

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal data held by us. They should:

- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested.
- Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified.
- Refer to the Data Protection Officer for assistance in demanding situations.
- Where providing information to a third party, do so in accordance with the data protection rules set out in this policy.

CCTV

In most countries, images of individuals fall within the definition of personal data because an individual can be identified from a video image. Some countries have specific legislation or guidance which sets out notification requirements and image retention time limits.

In accordance with our client agreements, AMS has CCTV in operation at all our GCSCs and our head office in London. Each office complies with its obligations relating to the collection of video images in accordance with the AMS Facilities Managers' CCTV Guidelines. Some of our other offices do not have CCTV in place.

TRAINING REQUIREMENTS

All AMS staff must complete mandatory Data Protection Training when first joining AMS, and annually thereafter. Where there are specific local or regional requirements and there is local or regional training this must be completed in line with specific regional requirements. Where client service staff are operating as data processors on behalf of clients, they should also complete client training where required by the client.

FURTHER ASSISTANCE

If you have any questions or concerns about the operation of this policy, please raise them with your line manager or the Data Protection Officer.

A|M|S

DOCUMENT CONTROL

Document Information

ITEM	
Title	AMS Data Protection Policy
Document Type	Policy
Document Status	Live
Document Classification	Internal
Author	Alistair Hay
Owner	Alistair Hay
Next Review Date	May 2027

Reviewer(s)

DATE REVIEWED	NAME – POSITION
29 August 2014	J Wainwright
22 October 2014	L Beck & J Wainwright
09 July 2015	S Beaumont – Data Protection Officer
27 June 2016	S Beaumont – Data Protection Officer
26 April 2018	A Hay – Data Protection Officer
May 2019	A Hay – Data Protection Officer
June 2020	A Hay – Data Protection Officer
March 2021	A Hay – Data Protection Officer
March 2022	A Hay – Data Protection Officer
March 2023	Michelle Kingston, Privacy Office Manager
March 2024	Michelle Kingston, Privacy Office Manager
May 2025	Michelle Kingston, Snr. Compliance Manager
May 2026	Michelle Kingston, Snr. Compliance Manager

A|M|S

Version Control

DATE ISSUED	VERSION	REASON FOR CHANGE	AUTHOR	APPROVED BY
18 August 2014	0.1	Original draft, issued for comment/review		
22 October 2014	0.2	Reflecting changes made following review		
09 July 2015	0.3	Reflecting changes made following review to make policy global in application and republished to reflect rebranding.		
27 June 2016	0.4	Updating to reflect declaration that Safe Harbour illegal.		
15 May 2018	1	Updated for GDPR	Alistair Hay	
21 May 2019	2	Annual update	Alistair Hay	
June 2020	3	Annual update	Alistair Hay	
March 2021	4	Branding update and inclusion of training requirements	Alistair Hay	
March 2022	5	Annual update	Alistair Hay	
March 2023	6	Annual Update	Michelle Kingston	Alistair Hay
March 2024	7	Annual Update	Michelle Kingston	Alistair Hay
May 2025	8	Annual Update	Michelle Kingston	Alistair Hay
May 2026	9	Annual Update	Michelle Kingston	Alistair Hay

Distribution

DATE DISTRIBUTED	VERSION	DISTRIBUTED TO
15/03/2023	V6	AMS Sharepoint, Risk, MyAMS, Privacy Office & Head of Compliance
07/03/2024	V7	AMS Sharepoint, Risk, MyAMS, Privacy Office & Head of Compliance

14/05/2025	V8	AMS Sharepoint, Risk, MyAMS, Privacy Office & Head of Compliance
20/05/2026	V9	AMS Sharepoint, Risk, MyAMS, Privacy Office & Head of Compliance

A|M|S

AMS Privacy Office

E/ dataprotection@weareAMS.com