ALVAREZ & MARSAL

Recruitment Privacy Notice Supplement (EU / EEA / UK / Switzerland)

Effective Date: January 1, 2026

This ***Recruitment Privacy Notice Supplement (EU / EEA / UK / Switzerland) ("European Recruitment Privacy Supplement"***) is provided to you by Alvarez & Marsal Holdings, LLC (**"*Holdings*"**) on behalf of itself and its subsidiaries, and any other professional services companies operating under the Alvarez & Marsal (or A&M) brand, that are established in the European Union, European Economic Area, United Kingdom and Switzerland (together, ***"A&M"***, ***"we"***, ***"our"***, ***"us"***).

This European Recruitment Privacy Supplement constitutes a Local Privacy Supplement as referred to in A&M's *Global Recruitment Privacy Notice*. It provides additional information to, and must be read in conjunction with, our Global Recruitment Privacy Notice. In the event of any conflict between this European Recruitment Privacy Supplement and A&M's Global Recruitment Privacy Notice, this European Recruitment Privacy Supplement will prevail.

This European Recruitment Privacy Supplement provides additional information regarding the following sections of the Global Recruitment Privacy Notice:

1) The controller of your personal information.
2) The categories of personal information we collect.
3) Our use of personal information.
4) Our lawful bases to process personal information.
5) Cross border transfers of personal information.
6) Your individual rights.
7) How to contact us.

As used herein, "***Applicable Data Protection Laws"*** specifically means all laws, rules and regulations of the European Union and its member states, European Economic Area member states, Switzerland, and United Kingdom applicable to the processing of personal information, including without limitation (i) EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council (***"GDPR"***); (ii) GDPR as transposed into UK national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, together with the Data Protection Act 2018, the Data (Use and Access) Act 2025 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (collectively, ***"UK GDPR"***); and (iii) the New Swiss Federal Act on Data Protection of 25 September 2020 (***"nFADP"***).

This European Recruitment Privacy Supplement does not constitute or form any part of an employment, directorship, ownership, partnership, independent contractor or any other type of agreement with us or confer any contractual right on you or place any contractual obligations on us. If you become an employee, officer, partner, independent contractor, or any other category of worker, you will be provided with our Global Workplace Privacy Notice and European Workplace Privacy Supplement, which supersedes this notice.

1. The Controller of Your Personal Information

Depending on the nature of the processing activity, the controller of your personal information will be (i) the local A&M entity considering you as a job applicant, (ii) our top-level entity within the country of your residence, if

different, (iii) Holdings (which is our top-level parent, located in the United States), and/or (iv) other Holdings subsidiaries and members of the A&M group.

Return to top of page.

2. Categories of Personal Information We Collect

All references to **"personal information"** in the *Global Recruitment Privacy Notice* and this European Recruitment Privacy Supplement shall be understood to refer exclusively to "personal data" as defined under GDPR Art. 4(1) and similar definitions under Applicable Data Protection Laws. Notwithstanding anything in the *Global Recruitment Privacy Notice* to the contrary, personal information includes publicly available information.

All references to **"sensitive personal information"** in the *Global Recruitment Privacy Notice* and this European Recruitment Privacy Supplement shall be understood to refer exclusively to (i) GDPR Art. 9(1) "**special categories of personal data**" (i.e., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, or sex life or sexual orientation), (ii) GDPR Art. 10 "**personal data relating to criminal convictions and offences**", and (iii) similarly defined terms under nFADP.

Return to top of page.

3. Use of Personal Information

A&M does not use your personal information for automated decision making, including profiling.

Return to top of page.

4. Lawful Bases to Process Personal Information

We process personal information for the purposes described in our *Global Recruitment Privacy Notice*. Please refer to **Annex 1** to this European Recruitment Privacy Supplement for additional information on our legal bases for processing.

Return to top of page.

5. Cross Border Transfers of Personal Information

A&M is a global company with offices around the world and with its parent company located in the United States. Except where prohibited by (and subject to the requirements of) Applicable Data Protection Laws, A&M may transfer your personal information outside the country where you are located (which may be the country of your residence or your primary A&M office) to other countries or territories where A&M, its service providers, or other third parties are located, including to countries or territories outside the European Union ("**EU**"), European Economic Area ("**EEA**"), UK and Switzerland whose laws have not been determined to provide an adequate level of protection for the processing of personal information as compared to Applicable Data Protection Laws, for the purposes set out in A&M's *Global Recruitment Privacy Notice*.

Internal Transfers

When we transfer your personal information within the A&M group to countries or territories outside the EU, EEA, UK and Switzerland that have not been determined to provide an adequate level of protection for the processing of personal information as compared to Applicable Data Protection Laws, it is pursuant to a companywide Intra-Group Personal Data Sharing and Transfer Agreement that incorporates GDPR Art. 46(2)(c) standard contractual clauses

approved by the European Commission, UK Information Commissioner, and Swiss Federal Data Protection and Information Commissioner ("**SCCs**").

External Transfers

When we transfer your personal information to third parties (including, but not limited to, processors such as our talent network and job application platform) located in countries or territories outside the EU, EEA, UK and Switzerland that have not been determined to provide an adequate level of protection for the processing of personal information as compared to Applicable Data Protection Laws, it is our policy to ensure that recipients are bound to maintain appropriate levels of data protection, security and confidentiality, and to comply with the requirements of GDPR Art. 44-50 (and similar requirements) for transfers of personal information outside the jurisdiction in which it was originally collected.

Wherever personal information is transferred to third parties outside of the EU, EEA, Switzerland and/or the UK, we will utilise any necessary and appropriate safeguards including the EU-US Data Privacy Framework adopted pursuant to European Commission Implementing Decision of 10 July 2023 (as well as the UK Extension to the EU-US Data Privacy Framework adopted pursuant to The Data Protection (Adequacy) (United States of America) Regulations 2023 and any analogous frameworks or certification schemes adopted by the applicable governmental or regulatory body under Applicable Law), SCCs, or on occasion, where relevant and permissible, derogations under GDPR Art. 49 or equivalent provision under Applicable Data Protection Laws (including the UK GDPR and as adapted to also satisfy Swiss law requirements). For certain ad hoc transfers, we may rely on other exemptions such as the transfer is necessary for the performance of a contract with you. In general, we do not rely on such derogations but may do so where there is a clear lawful basis.

Return to top of page.

6. Individual Rights

You have specific rights under Applicable Data Protection Laws regarding the personal information we collect and process about you. These rights are designed to give you greater transparency and control over your personal information. In particular, you have the following rights:

(1) Right to be Informed (GDPR Art. 13, 14). You have the right to be informed about the collection and use of your personal information. A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement, is part of our commitment to transparency.

(2) Right of Access (GDPR Art. 15). You may request access to the personal information we hold about you.

- ✓ Please note: The right of access is subject to certain limitations and exemptions. Reasons that we may restrict access to personal information include, without limitation, where disclosure would adversely affect the rights and freedoms of others, or where disclosure would breach another individual's privacy rights; be subject to legal professional privilege, meaning communications between you and legal advisors or between us and our legal counsel may be exempt; interfere with ongoing investigations, disciplinary proceedings, or regulatory functions; be restricted under national laws or statutory obligations, such as those related to crime prevention, taxation, or public health; involve confidential references provided for employment or training purposes; be part of management forecasting or planning, where disclosure would prejudice the conduct of the business; or relate to negotiations with you, where disclosure would prejudice those negotiations.

We will assess each request on a case-by-case basis and inform you if any exemptions apply, along with the reasons for withholding any information.

(3) Right to Rectification (GDPR Art. 16). If any of your personal information is inaccurate or incomplete, you have the right to request that it be corrected or updated.

(4) Right to Erasure ("Right to be Forgotten") (GDPR Art. 17). In certain circumstances, you may request the deletion of your personal information, specifically:

(i) *Data No Longer Necessary*. The personal information is no longer necessary for the purposes for which it was originally collected or otherwise processed.

(ii) *Withdrawal of Consent*. You withdraw your consent on which the processing is based, and there is no other legal ground for the processing.

(iii) *Objection to Processing*. You object to the processing of your data: (a) GDPR Art. 21(1) (based on legitimate interests), and there are no overriding legitimate grounds for the processing, or (b) under GDPR Art. 21(2) (for direct marketing purposes).

(iv) *Unlawful Processing*. The personal information has been unlawfully processed in breach of Applicable Data Protection Laws.

(v) *Legal Obligation*. The personal information must be erased to comply with a legal obligation under EU law, EU or EEA member state law, UK law, or Swiss law to which A&M is subject.

If your personal information has been made public and we are required to erase it, we will take reasonable steps, including technical measures, to inform other controllers processing the data that you have requested the erasure of any links to, or copies or replications of, that data.

✓ Please note: The right of erasure is not absolute. We may refuse your request where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation or for the performance of a task carried out in the public interest; for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research, or statistical purposes, where erasure would seriously impair the achievement of the objectives of that processing; and for the establishment, exercise, or defense of legal claims.

(5) Right to Restrict Processing (GDPR Art. 18). You may request that we restrict the processing of your personal information in specific situations, such as when you contest the accuracy of the data or object to its processing.

(6) Right to Data Portability (GDPR Art. 20). Where applicable, you have the right to receive your personal information in a structured, commonly used, and machine-readable format and to transmit that data to another controller.

(7) Right to Object (GDPR Art. 21). You have the right to object to the processing of your personal information in certain circumstances, including processing based on legitimate interests or for direct marketing purposes.

(8) Rights in Relation to Automated Decision-Making and Profiling (GDPR Art. 22). You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects. Automated decision-making with legal or similarly significant effects on the basis of sensitive personal information is permissible only with your explicit consent or where necessary for reasons of substantial public interest. As noted above, A&M does not use your personal information for automated decision making, including profiling.

✓ Please note: The right not to be subject to automated decision making is not absolute. We may engage in automated decision making, including profiling, where the processing is either necessary for entering into or performing a contract between us and you, authorized by law (e.g., for purposes of detecting fraud), or based on your explicit consent.

(9) Right to Withdraw Consent (GDPR Art. 7(3)). If we are processing your personal information based on your consent, you have the right to withdraw consent at any time. Please note, any such withdrawal of consent will not affect the lawfulness of our processing based on consent before such withdrawal.

(10) Right to Lodge a Complaint. If you believe your data protection rights have been violated, you have the right to lodge a complaint with the relevant supervisory authority.

A&M will make reasonable efforts to accommodate your requests, but A&M is under no obligation to honor any specific request absent a legal requirement. If we cannot honor your request or are under no legal obligation to do so, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

To exercise any of your privacy rights, or to submit any request or complaint regarding the processing of your personal information, please contact us in writing using any of the contact methods provided in **Section 7**.

Please note, to help protect your privacy and maintain security, we may take steps to verify your identity before complying with your request. For example, we may require you to provide your name, additional contact details, and the nature of your relationship with A&M. In addition, if you ask us to provide you with specific pieces of personal information or to delete information that we deem to be sensitive, we may require you to sign a declaration under penalty of perjury that you are the data subject whose personal information is the subject of the request. If you designate an authorized agent to exercise your privacy rights on your behalf, we may require proof (your signed permission) demonstrating that you authorized the agent to act on your behalf; and, further, we may require you to verify your own identity and confirm that you authorized the agent to submit the request on your behalf. We may deny any request submitted by an agent that does not meet these requirements. We may charge you a fee to access your personal information; however, we will notify you of any fee in advance.

Return to top of page.

7. Contact Us

To exercise any of your individual rights, or to submit any request or complaint regarding our processing of your personal information, please contact us at:

Talent Acquisition	talentacquisition@alvarezandmarsal.com
Webform	Available through A&M's Website Privacy Notice ("Individual Rights") ***(here).***

Return to top of page.

ANNEX 1

Legal Grounds for Processing Personal Information

Personal information: A&M processes your personal information on the following lawful bases, as further specified in Annex 1 to our *Global Recruitment Privacy Notice*:

- Contract
- Legal obligation
- Legitimate interests
- Vital interests
- Consent

Sensitive personal information: A&M processes your sensitive personal information for the purposes specified in our *Global Recruitment Privacy Notice* only if (in addition to having a lawful basis) one of the following special conditions or other legally permitted derogation applies:

- You have given your explicit consent.
- Processing being necessary for the purposes of your or our obligations and rights in relation to employment, in so far as it is authorised by law or collective agreement.
- Processing is necessary to protect your or another person's vital interests where you or the other person is physically or legally incapable of giving consent.
- Processing relating to data about you that you have made public (e.g., posted to publicly available social media).
- Processing is necessary for the purpose of establishing, making or defending legal claims.
- Processing being necessary for the assessment of your working capacity.
- Processing is necessary for reasons of substantial public interest, e.g., equality and diversity purposes to the extent permitted by law. You may be asked to provide diversity or other equal opportunities employment information as part of your application; however, you are not required to provide any such information, and should you decide not to provide such information your application to A&M will not be affected in any way. Any information you do provide will be used only to produce and monitor equal opportunities statistics.

In addition, in certain countries, our processing of your sensitive personal information is subject to further special conditions. Please see **Annex 2** (country annexes) and **Annex 3** (UK only) for details.

For information regarding of your country's data protection regulator please see **Annex 4.**

Return to top of page.

ANNEX 2

Country Annexes

ANNEX 2-A

Austria Notice – Applicable to job applicants in Austria

Any workplace CCTV or access-control systems we use will comply with Applicable Data Protection Laws and Austrian labour law with appropriate written policies, including clear and prominent transparency, strict purpose limitation and necessity, and retention limited to what is strictly required to achieve the stated purposes. Where the deployment of such systems is likely to result in a high risk to employees' rights and freedoms, we will carry out a data protection impact assessment before implementation.

Personal information relating to criminal convictions and offences will be processed only where permitted by Applicable Data Protection Laws and justified by the nature of the role or a clear legal requirement, and with appropriate safeguards. We will not rely on consent where it is not freely given.

Please contact Human Resources or our Privacy Office as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-B

Belgium Notice – Applicable to job applicants in Belgium

We will ask you only for information that is strictly necessary for the role. If we wish to obtain information from third parties (e.g., references), we will first inform you and, where required, obtain your written authorisation unless you have proactively identified the referee in your application materials.

Any CCTV, access-control, or electronic communications monitoring we carry out is limited to the purposes, transparency and proportionality requirements set out in Applicable Data Protection Laws and is preceded by a data-protection-impact assessment where required.

Where permitted based on the nature of your role, and subject to the requirements of Applicable Data Protection Laws and applicable local laws, including where applicable with respect to your prior consent, A&M and/or a third party acting on our behalf may process personal information relating to criminal convictions and offences in connection with a pre-hire background check or the investigation of fraud.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-C

Denmark Notice – Applicable to job applicants in Denmark

Where permitted based on the nature of your role, and subject to the requirements of Applicable Data Protection Laws and applicable local laws, including where applicable with respect to your prior consent, A&M and/or a third party acting on our behalf may process personal information relating to criminal convictions and offences in connection with a pre-hire background check or the investigation of fraud.

We process Civilt Personregister (Civil Registration Register) numbers only where required by law, with your consent, or where clearly justified by a legitimate interest that overrides your privacy interests (e.g., tax reporting, statutory employment filings). Where we must transmit special-category or otherwise confidential data by e-mail, we use end-to-end encryption in accordance with Danish Data Protection Agency ("**Datatilsynet**") guidance.

Unsuccessful candidate data is deleted no later than three years after the recruitment process ends.

In exceptional cases the Datatilsynet may restrict or prohibit the transfer of special-category data to third-country recipients even where a standard transfer mechanism exists. A&M will notify you if such a restriction affects your data.

You have the right to give us specific instructions regarding your personal information for up to ten years after your death.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-D

France Notice – Applicable to job applicants in France

You have a right to data portability, where we are relying on your consent or performance of a contract: you may request to receive, in a structured and commonly used format, all your personal information processed by automated means. You may also request that we transfer these data directly to another organization.

You also have the right to give us specific instructions on what to do with your personal information after your death.

Where permitted based on the nature of your role, and subject to the requirements of Applicable Data Protection Laws and applicable local laws, including where applicable with respect to your prior consent, A&M and/or a third party acting on our behalf may process personal information relating to criminal convictions and offences in connection with a pre-hire background check or the investigation of fraud.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-E

Germany Notice – Applicable to job applicants in Germany

A&M's German external data protection officer (DPO) is as follows:

Dr. Felix Wittern
Fieldfisher Tech Rechtsanwaltsgesellschaft mbh
Am Sandtorkai 68
20249 Hamburg
Germany
felix.wittern@fieldfisher.com
Tel: +49 (0)40 878 869 81 14

Please note that the legal basis for the "Performance of a contract" is – in Germany – § 26 (1) German Federal Data Protection Act (Bundesdatenschutzgesetz).

The lawful basis for processing background check data is your consent.

Application data will be deleted after 6 months ((i) if you have not given consent for a longer storage period or (ii) unless we need the data for legal proceedings)

Equal opportunities monitoring does not take place in your country.

Where permitted based on the nature of your role, and subject to the requirements of Applicable Data Protection Laws and applicable local laws, including where applicable with respect to your prior consent, A&M and/or a third party acting on our behalf may process personal information relating to criminal convictions and offences in connection with a pre-hire background check or the investigation of fraud.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-F

Netherlands Notice – Applicable to job applicants in The Netherlands

Where permitted based on the nature of your role, and subject to the requirements of Applicable Data Protection Laws and applicable local laws, including where applicable with respect to your prior consent, A&M and/or a third party acting on our behalf may process personal information relating to criminal convictions and offences in connection with a pre-hire background check or the investigation of fraud.

In addition, sensitive personal information will in principle not be processed, unless we are allowed to do so under the GDPR and the Dutch Implementation Act to the GDPR (UAVG). This is only for specific exceptions and limited circumstances and we will strictly adhere to the requirements under the UAVG. The same applies for the processing of criminal data.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-G

Portugal Notice – Applicable to job applicants in Portugal

We may process biometric data solely for attendance or access-control purposes, and only where necessary, proportionate and accompanied by appropriate technical and organisational safeguards.

Any monitoring technologies deployed while you work remotely (e.g., VPN logs) will be limited to what is strictly necessary for security, time-keeping or resource-allocation purposes and will comply with Portuguese labour-law restrictions.

Images captured through CCTV or other remote-surveillance technologies will be used only for purposes permitted under Article 20 of the Labour Code.

In addition, sensitive personal information will in principle not be processed, unless we are allowed to do so under Applicable Data Protection Laws and applicable local laws. This is only for specific exceptions and limited circumstances, and we will strictly adhere to these legal requirements. The same applies for the processing of criminal data.

With the limited exception of disability information, equal opportunities monitoring does not take place in your country.

After your death, your heirs or persons you designate may exercise certain rights of access, rectification and erasure over your personal information, subject to proof of status and our legitimate-interest and legal-retention obligations.

You may exercise the right to erasure only once mandatory statutory retention periods have expired.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-H

Switzerland Notice – Applicable to job applicants in Switzerland

Please note that payroll data may also consist of data about your religious belief. The lawful basis for processing is compliance with Swiss statutory law (nFADP Art. 4, 12, 13, 14).

Where permitted based on the nature of your role, and subject to the requirements of Applicable Data Protection Laws and applicable local laws, including where applicable with respect to your prior consent, A&M and/or a third party acting on our behalf may process personal information relating to criminal convictions and offences in connection with a pre-hire background check or the investigation of fraud.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

Return to top of page.

ANNEX 2-I

UK Notice – Applicable to job applicants in the UK

We carry out equal opportunities monitoring in the UK in connection with talent acquisition and human resources, and we may report our statistics to government agencies. The lawful basis for processing equal opportunities data is that it is in the substantial public interest to monitor equality. It is in A&M's legitimate interests to ensure that we have a diverse workforce and that there is no discrimination in hiring.

Our Appropriate Policy Document, setting out how sensitive personal information is processed, follows at Annex 3.

Where permitted based on the nature of your role, and subject to the requirements of Applicable Data Protection Laws and applicable local laws, including where applicable with respect to your prior consent, A&M and/or a third party acting on our behalf may process personal information relating to criminal convictions and offences in connection with a pre-hire background check or the investigation of fraud.

Please contact us as specified in Section 7 of this European Recruitment Privacy Supplement to resolve any questions about the processing we carry out on your personal information or request information about your privacy.

You have the right to submit a complaint to us about how we process your personal information. If you would like to exercise this right, please Talent Acquisition as specified in Section 7 of this Recruitment Privacy Notice Supplement.

Return to top of page.

ANNEX 3

UK Appropriate Policy Document – Applicable to job applicants in the UK

Please note that A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement (including the information detailed below), along with other related policies and/or protocols, shall form our policy for processing special categories of personal information and criminal convictions data as required by the UK Data Protection Act 2018 (Schedule 1 Part IV).

Description of special data processed:

- Nationality, racial and ethnic origin, gender, sexual orientation, religion, disability, age, and data concerning health.
- Criminal convictions data, as part of the hiring process for certain roles.

Schedule 1 conditions for processing:

- Processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller in connection with employment (Schedule 1, Part I, section 1 UK Data Protection Act 2018);
- Processing is necessary for reasons of substantial public interest relating to equality of opportunity or treatment (Schedule 1, Part II, section 8(1) UK Data Protection Act 2018); and
- Processing is necessary for reasons of substantial public interest relating to racial and ethnic diversity at senior levels (Schedule 1, Part II, section 9(1) UK Data Protection Act 2018).

Procedures for ensuring compliance with the principles:

- **Accountability principle:**
    - We maintain appropriate documentation of our processing activities, as set out in our Article 30 record of processing.
    - We have appropriate data protection policies in place, such as the Global Data Protection Policy, Workforce Security Policy, and related policies, guidelines and documents.
    - We carry out data protection impact assessments (DPIA) for uses of personal information that are likely to result in high risk to individuals' interests.
- **Principle (a): lawfulness, fairness and transparency:**
    - We identify an appropriate lawful basis for processing and a further Schedule 1 condition for processing special data, as set out in A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement.
    - We make appropriate privacy information available with respect to the special data, as set out in A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement.
    - We are open and honest when we collect the special data and we ensure we do not deceive or mislead people about its use, by making A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement, available.
- **Principle (b): purpose limitation:**
    - We have clearly identified our purposes for processing the special data, as set out in A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement.

- We have included appropriate details of these purposes in our privacy information for individuals, as set out in A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement.
- If we plan to use personal information for a new purpose (other than a legal obligation or function set out in law), we either check that this is compatible with our original purpose or where we have another lawful basis, be transparent about this new processing or get specific consent for the new purpose.

- **Principle (c): data minimisation:**
  - We are satisfied that we only collect special data that we actually need for our specified purposes.
  - We are satisfied that we have sufficient special data to properly fulfil those purposes.
  - We periodically review this data and delete anything we don't need.
- **Principle (d): accuracy:**
  - We have appropriate processes in place to check the accuracy of the special data we collect, and we record the source of that data.
  - We have a process in place to identify when we need to keep the special data updated to properly fulfil our purpose, and we update it as necessary.
- **Principle (e): storage limitation:**
  - We carefully consider how long we keep the special data, and we can justify this amount of time.
  - We regularly review our information and erase or anonymise this special data when we no longer need it.
- **Principle (f): integrity and confidentiality (security):**
  - We have analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data.
  - We have policies, including A&M's *Global Recruitment Privacy Notice*, together with this European Recruitment Privacy Supplement, and other A&M policies and procedures maintained by the Global Security Office, Information Technology (HRIS), Human Resources and Talent Acquisition, regarding this special data, and we take steps to make sure these policies are implemented. Each is reviewed regularly.
  - We have put other technical measures or controls in place because of the circumstances and the type of special data we are processing.

Retention and erasure policies

We are committed to the security of special categories of personal information and criminal convictions data that we hold. We have administrative, physical, and technical safeguards in place to protect personal information against unlawful or unauthorised processing, or accidental loss or damage. We will ensure where special categories of personal information or criminal convictions data are processed that:

- The processing is recorded, setting out, where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our data retention policy.
- Where we no longer require special categories of personal information or criminal convictions data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as practicable.
- Where records are destroyed, we will ensure that they are safely and permanently disposed of.

A&M maintains record retention schedules that set out the criteria used to determine the period for which personal information is stored. You may request information concerning these retention periods, as set out in the main body of A&M's *Global Recruitment Privacy Notice* and European Recruitment Privacy Supplement.

Return to top of page.

ANNEX 4

Supervisory Authorities

Jurisdiction	Regulator
Austria	**Austrian Data Protection Authority** https://data-protection-authority.gv.at/
Belgium	**Belgian Data Protection Authority** https://www.dataprotectionauthority.be/citizen
Czech Republic	**Office for Personal Data Protection** https://uoou.gov.cz/en
Denmark	**The Danish Data Protection Agency** https://www.datatilsynet.dk/english
Finland	**The Office of the Data Protection Ombudsman** https://tietosuoja.fi/en/home
France	**Commission nationale de l'informatique et des libertés (CNIL)** https://www.cnil.fr/en/home
Germany	**The Federal Commissioner for Data Protection and Freedom of Information (BfDI)** https://www.bfdi.bund.de/EN/Home/home_node.html **Data protection authorities of the federal states** https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html
Greece	**The Hellenic Data Protection Authority** https://www.dpa.gr/en
Ireland	**Data Protection Commissioner** https://www.dataprotection.ie/en
Italy	**Italian Data Protection Authority (Garante)** https://garanteprivacy.it/web/garante-privacy-en/home_en
The Netherlands	**Dutch Data Protection Authority (AP)** https://autoriteitpersoonsgegevens.nl/en
Norway	**The Norwegian Data Protection Authority (Datatilsynet)** https://www.datatilsynet.no/en/
Poland	**The Office for Personal Data Protection (UODO)** https://uodo.gov.pl/en
Portugal	**Portuguese Data Protection Authority (CNPD)** https://www.cnpd.pt/
Romania	**National Supervisory Authority for Personal Data Processing (ANSPDCP)** https://www.dataprotection.ro/
Spain	**Spanish Data Protection Agency (AEPD)** https://www.aepd.es/
Sweden	**The Swedish Data Protection Agency (IMY)** https://www.imy.se/en/
Switzerland	**The Federal Data Protection and Information Commissioner (FDPIC)** https://www.edoeb.admin.ch/en
UK	**Information Commission (IC)** https://ico.org.uk/

[End]