

Privacy Policy

Right to Object:

You have a legal right to object at any time to:(i) use of your personal information for direct marketing purposes; and(ii) processing of your personal information which is based on our legitimate interests, unless there are compelling legitimate ground for our continued processing.

1. Introduction

This Policy sets out the obligations of Team A5 Limited(“Team A5”, “the company”, “we”, “us” or “our”), a company registered in England under number 09364084 whose registered office is at First Floor 792-794 London Road | Thornton Heath Croydon | CR7 6JB | United Kingdom regarding data protection and the rights of candidates, clients, all internal & external stakeholders & users of our website.

(“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 Team A5 Limited’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 Team A5 Limited, its employees, agents, contractors, or other parties working on behalf of the Company.

Team A5 Limited 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.

2. 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:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. 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.

3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. 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.
5. 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.
6. 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.

7.

The Information We Collect and How We Use It

Team A5 Limited may collect your personal details, including but not limited to your name and contact details (together with your e-mail address) and other relevant information from your CV. On occasions this may also include – sensitive personal information such as details of criminal convictions and ethnic origin. This information is held, used and disclosed by us as follows:

1. to provide our services to you;
2. to maintain our business relationship;
3. to enable you to submit your CV for general applications, to apply for specific jobs or to subscribe to our job alerts.
4. to match your details with job vacancies, to assist us in finding a position that is most suitable for you and to send your personal information (including sensitive personal information, when consent is provided) to clients in order to get you work;

5. to answer your enquiries;
6. to direct-market services, advise you of news and industry updates, events, reports and other information. Where we do so, you will be able to unsubscribe from such communications;
7. to fulfil contractual obligations with our clients.
8. to trusted third parties where we have retained them to provide services that you or our clients have requested, such as reference, qualification and criminal reference checking services (as required), verification of the details you have provided from third party sources, psychometric evaluations or skills tests. These third parties comply with similar and equally stringent undertakings of privacy and confidentiality as Team A5 Limited;
9. to third parties who perform functions on our behalf and who also provide services to us, such as professional advisors, IT consultants carrying out testing and development work on our business technology systems, Umbrella companies and function co-ordinators. These third parties comply with similar undertakings of privacy and confidentiality as Team A5 Limited Limited;
10. we may also release personal information to regulatory or law enforcement agencies, if they require us to do so. We will also disclose your information where we are permitted and requested to do so by law; and
11. we may also seek your consent to collect, hold, use and disclose your personal information for any other purpose not listed above.
12. our website may also use a website recording service which can record mouse clicks, mouse movements, page scrolling and any text keyed into website forms. Data collected by this service is used to improve our website usability. The information collected is stored and is used for aggregated and statistical reporting, and is not shared with anybody else.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

1. The right to be informed;
2. The right of access;

3. The right to rectification;
4. The right to erasure (also known as the 'right to be forgotten');
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. Rights with respect to automated decision-making and profiling.
- 9.

4. Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

1. The data subject has given consent to the processing of their personal data for one or more specific purposes;
2. The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
3. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
4. The processing is necessary to protect the vital interests of the data subject or of another natural person;
5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
7. [If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:
 - The data subject has given their explicit consent to the processing of such data for one or more specified purposes

(unless EU or EU Member State law prohibits them from doing so);

- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against

serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.]

•

5. Specified, Explicit, and Legitimate Purposes

1. Team A5 Limited collects and processes the personal data set out in Part 20 of this Policy. This includes:
 - Personal data collected directly from data subjects OR [; and]
 - Personal data obtained from third parties. OR [; and]
 - Personal data collected electronically, this may be through a direct application on our website or an application that data subjects have made through a third party job board.
2. Team A5 Limited only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).
3. Data subjects are kept informed at all times of the purpose or purposes for which Team A5 Limited uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

4.

5. Adequate, Relevant, and Limited Data Processing

Team A5 Limited will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data

subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Up-to-Date

1. Team A5 Limited shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.
2. The accuracy of personal data shall be checked when it is collected and at [regular] intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

1. Team A5 Limited shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

9. Secure Processing

Team A5 Limited shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

1. Team A5 Limited Data Protection Officer is Will Hobson, Contact Details: 020 7407 6620, GDPR@ep-healthcare.co.uk
2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.
3. Team A5 Limited shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
 - The name and details of Team A5 Limited, its Data Protection Officer, and any applicable third-party data processors;

- The purposes for which Team A5 Limited collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by Team A5 Limited, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company; and
- Detailed descriptions of all technical and organisational measures taken by Team A5 Limited to ensure the security of personal data.
-

11. Data Protection Impact Assessments

1. Team A5 Limited shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data [which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR].
2. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
 - The type(s) of personal data that will be collected, held, and processed;
 - The purpose(s) for which personal data is to be used;
 - The Company's objectives;
 - How personal data is to be used;
 - The parties (internal and/or external) who are to be consulted;
 - The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
 - Risks posed to data subjects;
 - Risks posed both within and to Team A5 Limited; and
 - Proposed measures to minimise and handle identified risks.
 -

12. Keeping Data Subjects Informed

Team A5 Limited shall provide the information set out in Part 12 (3) to every data subject:

1. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
2. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
 - if the personal data is used to communicate with the data subject, when the first communication is made; or
 - if the personal data is to be transferred to another party, before that transfer is made; or
 - as soon as reasonably possible and in any event not more than one month after the personal data is obtained.
3. The following information shall be provided:
 - Details of Team A5 Limited including, but not limited to, the identity of its Data Protection Officer;
 - The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
 - Where applicable, the legitimate interests upon which Team A5 Limited is justifying its collection and processing of the personal data;
 - Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
 - Where the personal data is to be transferred to one or more third parties, details of those parties;
 - Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
 - Details of data retention;
 - Details of the data subject’s rights under the GDPR;
 - Details of the data subject’s right to withdraw their consent to Team A5 Limited processing of their personal data at any time;

- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

•

13. Data Subject Access

1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Team A5 Limited holds about them, what it is doing with that personal data, and why.
2. Data subjects wishing to make a SAR may do so in writing, using Team A5 Limited Subject Access Request Form, or other written communication. SARs should be addressed to Team A5 Limited Data Protection Officer at GDPR@teama5.co.uk
3. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
4. All SARs received shall be handled by Team A5 Limited Data Protection Officer.
5. Team A5 Limited does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

1. Data subjects have the right to require Team A5 Limited to rectify any of their personal data that is inaccurate or incomplete.
2. Team A5 Limited shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be

extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

1. Data subjects have the right to request that Team A5 Limited erases the personal data it holds about them in the following circumstances:
 - It is no longer necessary for Team A5 Limited to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
 - The data subject wishes to withdraw their consent to Team A5 Limited holding and processing their personal data;
 - The data subject objects to Team A5 Limited holding and processing their personal data (and there is no overriding legitimate interest to allow Team A5 Limited to continue doing so);
 - The personal data has been processed unlawfully;
 - The personal data needs to be erased in order for Team A5 Limited to comply with a particular legal obligation OR
 - The personal data is being held and processed for the purpose of providing information society services to a child.
2. Unless Team A5 Limited has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
3. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

1. Data subjects may request that Team A5 Limited ceases processing the personal data it holds about them. If a data subject makes such a

request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

1. Team A5 Limited processes personal data using automated means on Eclipse (for agency workers & clients) and BrightHR (for employees)TBC
2. Where data subjects have given their consent to Team A5 Limited to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between Team A5 Limited and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
3. To facilitate the right of data portability, Team A5 Limited shall make available all applicable personal data to data subjects in the following format [s]:
 - Hard copy documents (employees only, no hard copies available for agency workers & clients);
 - Electronic files.
 - Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
 - All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. Objections to Personal Data Processing

1. Data subjects have the right to object to Team A5 Limited processing their personal data based on legitimate interests, direct marketing

(including profiling) and processing for scientific and/or historical research and statistics purposes.

2. Where a data subject objects to Team A5 Limited processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
3. Where a data subject objects to Team A5 Limited processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.
4. Where a data subject objects to Team A5 Limited processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". Team A5 Limited is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Personal Data Collected, Held, and Processed

Team A5 Limited collects the information necessary to be able to match data subjects with available job opportunities and also further information needed to assess data subjects' eligibility through the different stages of recruitment. This information includes CVs, identification documents, educational records, work history, employment and references. We may also collect sensitive personal data about candidates, in the form of health data for example. The company only collects sensitive personal data from data subject, and further process this data, where consent has been given. The following personal data is collected, held, and processed by Team A5 Limited:

Data Ref.	Type of Data	Purpose of Data
Interviews	Notes, handwritten & electronic, emails	Tracking of candidates
Passports	Passport scans or Photos	Compliance with regulations
Personal Details	Phone numbers, next of kin details & bank details	To ensure all information for emergency. Bank details for salary payments.

Data Ref.	Type of Data	Purpose of Data
Candidate Details	Phone numbers, email, & other contact details, address details other personal info.	To ensure all candidates currently opted in
Candidate CV'S	Work history & experience	To ensure we provide experience
Client Job Details	Handwritten or hard copies of Job specifications	To understand the candidates for the
Eclipse Database	All candidate data including but not exclusive to hourly rates, work history & career paths.	To ensure we understand

20. Data Security – Transferring Personal Data and Communications

Team A5 Limited shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

1. All emails containing personal data must be encrypted
2. All emails containing personal data must be marked “confidential”;
3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
4. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
5. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated there with should also be deleted;
6. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
7. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient [or sent using 1st class postal service or hand delivered.]
8. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

21. Data Security – Storage

Team A5 Limited shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords and data encryption;
2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.
3. All personal data stored electronically should be backed up weekly with backups stored offsite. All backups should be on-premises servers and the data is sent over a secure HTTPS link.
4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Team A5 Limited or otherwise.
5. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Team A5 Limited where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

22. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

23. Data Security – Use of Personal Data

Team A5 Limited shall ensure that the following measures are taken with respect to the use of personal data:

1. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Team A5 Limited requires access to any personal data that they do not already have access to, such access should be formally requested. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Data Protection Officer; Dulcie Jenner-Wilson
“GDPR@ep.adamscreative.co.uk”.

2. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
3. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
4. Where personal data held by Team A5 Limited is used for marketing purposes, it shall be the responsibility of Data Protection Officer; Will Hobson GDPR@teama5.co.uk to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

24. Data Security – IT Security

Team A5 Limited shall ensure that the following measures are taken with respect to IT and information security:

1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. [All software used by the Company is designed to require such passwords.];
2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Team A5 Limited, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT company do not have access to passwords;

25. Organisational Measures

Team A5 Limited shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

1. All employees, agents, contractors, or other parties working on behalf of Team A5 Limited 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;
2. Only employees, agents, sub-contractors, or other parties working on behalf of Team A5 Limited 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;

3. All employees, agents, contractors, or other parties working on behalf of Team A5 Limited handling personal data will be appropriately trained to do so;
4. All employees, agents, contractors, or other parties working on behalf of Team A5 Limited handling personal data will be appropriately supervised;
5. All employees, agents, contractors, or other parties working on behalf of Team A5 Limited 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;
6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
7. All personal data held by Team A5 Limited shall be reviewed periodically;
8. The performance of those employees, agents, contractors, or other parties working on behalf of Team A5 Limited handling personal data shall be regularly evaluated and reviewed;
9. All employees, agents, contractors, or other parties working on behalf of Team A5 Limited handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
10. All agents, contractors, or other parties working on behalf of Team A5 Limited 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
11. Where any agent, contractor or other party working on behalf of Team A5 Limited handling personal 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.

26. Transferring Personal Data to a Country outside the EEA

1. The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
 - The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
 - The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
 - The transfer is made with the informed consent of the relevant data subject(s);
 - The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
 - The transfer is necessary for important public interest reasons;
 - The transfer is necessary for the conduct of legal claims;
 - The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
 - The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

27. Data Breach Notification

1. All personal data breaches must be reported immediately to Team A5 Limited Data Protection Officer.
2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
3. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
4. Data breach notifications shall include the following information:
 - The categories and approximate number of data subjects concerned;
 - The categories and approximate number of personal data records concerned;
 - The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
 - The likely consequences of the breach;
 - Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

28. Website

1. The Company's website uses a website recording service which can record mouse clicks, mouse movements, page scrolling and any text keyed into website forms. Data collected by this service is used to improve our website usability. The information collected is stored and is used for aggregated and statistical reporting, and is not shared with anybody else.
2. In order to provide the data subject with personalised content on our website, with more relevant communication in our emails, and with a tailored service from our consultants, we track and record usage and interaction with our website and emails. We employ a third party service provider to help us record, store and analyse this information

to determine how we might best deliver your engagement. We ensure that no personally identifiable attributes are recorded in this database and, other than our chosen service provider, we do not share this information with any other business or affiliate.

3. Job Alerts: To subscribe to job alerts emails, data subjects will be required to provide their name and e-mail address, which will be used for the purpose of keeping them informed, by e-mail, of the latest jobs in their nominated industry and to provide them with industry news and other information related to our services. Should the data subjects decide that they no longer wish to receive this information, unsubscribe links are provided in every job alert email that they receive.
4. Aggregate Information: The company gathers information and statistics collectively about all visitors to our website, for example:
 - which area users access most frequently; and/or
 - Which services users access the most.
 - The company only uses such data in the aggregate form. This information helps us determine what is most beneficial for our users and how we can continually improve our online services to create a better overall experience for our users.
5. Use of Cookies: Like most websites, when you visit the company's website we place cookies on your computer or other device. For the most part, these cookies are used to enable the website functionality, improve the user experience or help us to optimise our website, measure traffic and other internal management purposes. You can find out more about our use of cookies, including how to reject cookies, in our Cookies Policy.
6. Internet-based transfers: Given that the Internet is a global environment, using the Internet to collect and process personal data necessarily involves the transmission of data on an international basis. Unfortunately the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site via third party networks; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

7. How Do You Access And Update Your Personal Information? Your personal information is located on a server(s) operated by Adams Creative Group Ltd. Team A5 Limited provides you with the means to access, update, edit or delete the Registration Information and other personal information you have provided to us at any time on your own by going to your user account and changing or deleting your Registration Information and other personal information as desired. If you decide at any time that you do not want to receive any updates you have subscribed for just send an email message to GDPR@teama5.co.uk indicating your preference not to receive updates. If you are unsure whether we have a record containing your personal information and would like to confirm whether or not we do, please send an email to GDPR@teama5.co.uk indicating all email addresses which you may have given us.
8. How Is Your Personal Information Secured and Protected? Where Team A5 Limited considers it appropriate, we use encryption and/or authentication tools among other methods to protect certain web-based personal information. E-mails you send us are not necessarily secure when they are transmitted to us. If your communication is sensitive or includes confidential information such as a credit card number, you may want to provide it by post or via the telephone instead.
9. We instruct our employees with access to your personal information that it is to be used only in adherence with the principles set forth in this Privacy Policy and the laws applicable to each specific business. Employees who misuse customer personal information may be subject to disciplinary action.
10. What If We Change Our Privacy Policy? Team A5 Limited reserves the right to modify or supplement this Privacy Policy statement at any time. If we make any material change to this Privacy Policy, we will update this Site to include such changes and post a notice on our home page, for a period of 30 days, with a link to the updated Privacy Policy and will send out an email to all our web users. Please read any such notice and the new policy statement. If you return to this Site after a period of more than 30 days, please check this Privacy Policy to confirm that you are aware of the details of the most recent update. Your continued use of this Site after we post such notice and after sending out an email will constitute your

acceptance of the new terms and their application to your use of this Site and the personal information disclosed for such use, including personal information previously furnished us, as if they were the initial terms, and your consent to the use of your personal information as described in this privacy policy and elsewhere at our Website. However, we will seek your consent if we want to use your personal information for purposes other than those you have agreed to previously.

11. Website Links: This Site may contain links to other sites, including those of our business partners, vendors and advertisers. While we try to link only to sites that share our high standards and respect for privacy, please understand that we are not responsible for the content of, or the privacy practices employed by, other sites.
12. Account Removal: You can remove your account and all your data from our system, simply login and click here.

29. Implementation of Policy

This Policy shall be deemed effective as of 18th January 2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

30. Contact

If you have any enquires or if you would like to contact us about our processing of your personal information, including to exercise your rights as outlined above, please contact us either by email or letter to the following address:-

Email: GDPR@teama5.co.uk

Post: First Floor 792-794 London Road | Thornton Heath Croydon | CR7 6JB | United Kingdom

When you contact us, we will ask you to verify your identity.