

1. Introduction

The General Data Protection Regulation (GDPR) 2018 regulates the processing of data relating to individuals. This includes the obtaining, holding, using or disclosing of such data and covers computerised records as well as manual filing systems and card indexes.

The Company (ASI Recruitment Ltd) shall hold the minimum personal data necessary to enable it to perform its functions due to legitimate interests. All such data is confidential and needs to be treated with care, to comply with the law.

We recognise that the lawful and correct treatment of personal data is very important to successful operations and to maintaining customers' and employees' confidence in ourselves.

Any personal data which we collect, record or use in any way whether it is held on paper, on computer or other media shall have appropriate safeguards applied to it to ensure that we comply with the Act.

ASI Recruitment is registered with the Information Commissioner (ZA139178).

2. Legitimate Interests

ASI Recruitment Ltd, will, where appropriate and allowed by law, rely on 'legitimate interests' as a lawful basis for handling personal data.

In this case, 'Legitimate Interests' means the interests of ASI Recruitment Ltd, in how we conduct and manage our activities.

We might refer to legitimate interests when we want to use your information in a way that we believe will benefit ASI Recruitment Ltd and the services we provide, however, we cannot do something we think is in our legitimate interests if it causes undue harm to the person whose information we are using. We need to make sure we get the balance right in all cases and will let you know what our use of your data will mean for you.

ASI Recruitment Ltd will use information supplied by you to aid the recruitment process and associated administrative functions.

3. Summary of Principles

The Company is fully committed to adhering to the Principles of GDPR as set out in the Regulation.

In summary, the Principles state that personal data shall:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 individuals;

- 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.
- To comply with the law, information shall be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

3. Personal Data

Personal data is defined by GDPR as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

GDPR also defines “sensitive personal data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The Company only holds personal data which is directly relevant to its dealings with a given data subject in addition to any such other similar personal data, in each case, as above for the legitimate purpose of the Company fulfilling its business as, primarily, a recruitment company. That data will be held and processed in accordance with the data protection principles and with this Policy. ASI Recruitment Ltd will only store information once permission has been granted by the candidate to store their data, unless permission is granted vicariously under the Terms of Business of the CV hosting site.

4. ASI Recruitment Ltd Principles

In terms of GDPR, we are the ‘data controller’, and as such determine the purpose for which, and the manner in which, any personal data are, or are to be, processed. Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

All data processors and data controllers are responsible for ensuring that:

- Any personal data they hold, whether in electronic or paper format, is kept securely.
- Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

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

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

- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of GDPR and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under GDPR.
- All contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and GDPR.
- Where any contractor, agent, consultant, partner or other party working on behalf of the Company 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.

In accordance with Article 33, where a breach of GDPR has been recognised, individuals will be notified directly. A notifiable breach has to be report to the relevant supervisory authority within 72 hours of ASI Recruitment Ltd becoming aware of it.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

All company computers have a log in system and personal data is password protected, which allow only authorised staff to access personal data. Passwords on all computers are changed frequently. All personal and financial data is kept in a locked filing cabinet and can only be accessed by approved staff. When staff members are using the laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.

5. How We Use Your Data

We will not use data for a purpose other than those agreed by data subjects. If the data held by us are requested by external organisations for any reason, this will only be passed if data subjects explicitly consent. ASI Recruitment will pass your personal details onto clients on application of a position. Consent will be sought prior to this taking place. Also, external organisations must state the purpose of processing, agree not to copy the data for further use.

The Company will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed. The Company will

always put our logo on all paperwork, stating their intentions on processing the data and state if, and to whom, we intend to give the personal data.

We discourage the retention of data for longer than it is required. All personal data will be deleted or destroyed by us after six years from receiving said data has elapsed.

Under Article 15, all individuals that the Company hold data on have the right to obtain from the controller confirmation as to whether or not personal data concerning the individual is being processed, and, where that is the case, access to the personal data and following information;

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with a supervisory authority; and
- Where the personal data are not collected from the data subject, any available information as to their source.

Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual.

From time to time we will undertake direct marketing via email in relation to potential job opportunities. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith. To opt out of such communication, please reply with 'opt out' and all communication will be ceased immediately. Alternatively, please contact (01603) 621103.

6. Subject Rights

One of the rules under GDPR gives you the right to see certain information held about you.

Personal data is confidential, and access is restricted. Under Article 15 an individual has the right to request copies of all their personal data known as a subject access request (SAR).

In order to get a copy of their personal data, an individual has to make a request either verbally or in writing, provide sufficient information to identify themselves and the information they are seeking. Individuals can contact: Subject Access Request, ASI Recruitment Ltd, 5 Queen Street, Norwich, NR2 4SG, (01603) 621103 or Alex@ASIRecruitment.co.uk. ASI Recruitment Ltd will respond to the SAR within one month of receiving.

All SARs will be treated in the strictest confidence and will only be processed by authorised ASI Recruitment Ltd staff in order to locate the information and process the SAR. Only information which is considered to be personal data will be released under a SAR. The anonymity of other individuals or other information which is not considered to be personal data may be protected, as appropriate, by redaction or omission in accordance with Article 15.

In order to request information on behalf of another individual ASI Recruitment Ltd requires proof that you are acting with the authorisation of that individual. Therefore, some additional information is required.

You have a right to object to the way in which we process of your data. Where your data has been used for direct marketing this is an absolute right.

If you have any complaint or concern relating to how we have handled your personal data, you can contact the Data Protection Officer in the first instance. The Information Commissioner's Office has published guidance on raising a concern with an organisation.

Data Subjects may request that the ASI Recruitment Ltd erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- The data subject objects to the Company holding and processing their personal data and there is no overriding legitimate interest to allow the Company to continue doing so;
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless the Company 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 (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

7. Links to Other Websites

This Website may, from time to time, provide links to other websites. ASI Recruitment Ltd has no control over such websites and is in no way responsible for the content thereof. This Policy does not extend to your use of such websites. Users are advised to read the privacy policy or statement of other websites prior to using them.

8. Cookies and Website Data

This Website may place and access certain first party Cookies on your computer. First party cookies are those placed directly by ASI Recruitment Ltd via this Website and are used only by ASI Recruitment Ltd. ASI Recruitment Ltd uses Cookies to improve your experience of using the Website and to improve our range of services. ASI Recruitment Ltd has carefully chosen these Cookies and has taken steps to ensure that your privacy is protected and respected at all times.

By using this Website you may receive certain third party Cookies on your computer. Third party cookies are those placed by websites and/or parties such as Google or Facebook or any other than ASI Recruitment Ltd. Third party cookies are used on this Website for advertising etc. These cookies are not integral to the services provided by the Website.

All Cookies used by this Website are used in accordance with current UK and EU Cookie Law.

You can choose to enable or disable Cookies in your internet browser. Most internet browsers also enable you to choose whether you wish to disable all cookies or only third-party cookies. By default, most internet browsers accept

Cookies but this can be changed. For further details, please consult the help menu in your internet browser.

You can choose to delete Cookies at any time however you may lose any information that enables you to access the Website more quickly and efficiently including, but not limited to, personalisation settings.

It is recommended that you ensure that your internet browser is up-to-date and that you consult the help and guidance provided by the developer of your internet browser if you are unsure about adjusting your privacy settings.

9. Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date and will be updated and reviewed regularly.