Connaught Executive Search Ltd

Privacy Notice

This Privacy Notice was last updated on 21st May 2018.

We reserve the right to change this Privacy Notice at any time. Such changes, modifications, additions or deletions shall be effective immediately upon notice thereof, which may be given by means including, but not limited to, posting a notice and the revised Privacy Notice on the Connaught Executive website.

Click on the links below to jump to each section:

1. General Points

1.1 The Board of Directors and management of Connaught Executive Limited ("Connaught"), located at 61 Rivington Street, London EC3A 2QQ, are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Connaught collects and processes in accordance with the General Data Protection Regulation (GDPR).

1.2 Compliance with the GDPR is described by this notice and takes into consideration our connected processes and procedures.

1.3 The GDPR and this notice apply to all of Connaught's personal data processing functions, including those performed on clients', employees', suppliers' and partners' personal data, and any other personal data that Connaught processes from any source.

1.4 Our Data Protection Officer is responsible for reviewing our processes, procedures, policies and guidelines on a half-yearly basis in the light of any changes to Connaught's activities (as determined by management review) and to any additional requirements identified by means of data protection impact assessments.

1.5 This notice applies to all staff, suppliers and partners of Connaught, including outsourced suppliers and partners. Any breach of the GDPR will be dealt with under Connaught's disciplinary policy and in if a criminal offence has been committed, the matter will be reported as soon as possible to the appropriate authorities.

1.6 Partners and any third parties working with or for Connaught, and who have or may have access to personal data, will be expected to have read, understood and comply with this notice. No third party may access personal data held by Connaught without having first entered into a Data Security and Confidentiality Agreement, which imposes on the third-party obligations no less onerous than those to which Connaught is committed, and which gives Connaught the right to audit compliance with the agreement.

2. Responsibilities and roles under the General Data Protection Regulation

2.1 Connaught is a Data Controller under the GDPR.

2.2 Top Management and all those in managerial or supervisory roles throughout Connaught are responsible for developing and encouraging good information handling practices within Connaught; responsibilities are set out in individual job descriptions.

2.3 Connaught's Data Controller is Jessica Cooksey, who can be contacted by email at jessicacooksey@connaughtexec.com. Jessica has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the person that you should contact if you require any information or have any questions.

2.4 **Should you require a copy of your data, as prescribed by the GDPR, you can contact Jessica at** jessicacooksey@connaughtexec.com.

2.5 Connaught's Data Protection Officer is Andrew Brown CDPO, CIPP/E, of Nichcom Limited www.nichcom.co.uk. Andrew can be contacted at andy.brown@nichcom.co.uk. As required in the GDPR, he is an advisor to Connaught's Data Controller, is accountable to the Directors of Connaught for the management of personal data and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

2.5.1 development and implementation of the GDPR as required by this notice; and

2.5.2 security and risk management in relation to compliance with the policy.

2.6 Compliance with data protection legislation is the responsibility of all Employees/Staff of Connaught who process personal data.

2.7 Connaught's Training Policy sets out specific training and awareness requirements in relation to specific roles and of staff generally.

2.8 All staff at Connaught are responsible for ensuring that any personal data is accurate and up-to-date.

3. Data protection principles

3.1 All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Connaught's policies and procedures are designed to ensure compliance with the principles.

The GDPR states that:

3.2 Personal data must be processed lawfully, fairly and transparently

Lawful – Connaught initially acquires personal data from CVs that are posted in the public domain on various jobsites, job boards and forums. We then engage with data subjects via a telephone call, or by email. In both cases we ask for consent to keep a record of the personal data that is contained within the data subject's CV. Consent is reinforced by the contract for services which is put in place between Connaught and the data subject, in that it is necessary for Connaught to hold personal data in the performance of the contract for services, as set out in Article 6 1.(b) of the GDPR.

Fairly – Connaught will make certain information available to data subjects as soon as practicable following a request from the data subject. This applies whether the personal data was obtained directly from data subjects or from other sources.

Transparently – Connaught aim to provide all details about personal data and reasons for processing in a transparent way. If you are unclear about any aspects of our work or our policies, please get in touch with our Data Controller, who is mentioned in 2.3 above.

3.3 Personal data can only be collected for specific, explicit and legitimate purposes

Connaught use personal data for the following processing activities:

3.3.1 To assist individuals in their preparation for job searches or with any aspects of their personal career development;

3.3.2 To assist individuals with in aspects of their promotion and marketing to recruiters, headhunters and organisations seeking to hire;

3.3.3 To market our 'alumni' events, that connect individuals to their peers as well as to any third parties such as recruiters or potential employers.

Connaught do not process data for any other purposes than stated above.

3.4 Personal data must be adequate, relevant and limited to what is necessary for processing

3.4.1 Connaught only collect enough personal data from individuals as is necessary to perform the processing noted in 3.3 above.

3.4.2 All data collection forms and methods have been reviewed by our Data Protection Officer and have been deemed to be fair methods of collection.

3.4.3 Our Data Protection Officer will ensure that, on a half-yearly basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

3.5 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

3.5.1 Connaught's Data Controller will review and update data within our systems as necessary. No data is kept unless it is reasonable to assume that it is accurate.

3.5.2 Our Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

3.5.3 It is the responsibility of Connaught to ensure that any notification regarding changes of circumstances are recorded and acted upon.

3.5.4 Our Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

3.5.5 Connaught's Data Controller is responsible for responding to requests for rectification from data subjects within one month of the request. This can be extended to a further two months for complex requests, according to Article 12 3. of the GDPR. If Connaught decides not to comply with the data subject request, our Data Protection Officer will

respond to the data subject to explain the reasoning and inform the data subject of their right to complain to the supervisory authority and seek judicial remedy.

3.5.6 Connaught's Data Controller is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, they will be informed that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

3.6 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

3.6.1 We do not retain data past the periods prescribed by our Retention Policy and our Retention Schedule.

3.6.2 Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it will be securely destroyed as set out in this procedure.

3.6.3 Our Data Protection Officer will specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure, and will ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval will be made in writing.

3.7 Personal data must be processed in a manner that ensures the appropriate security

Our Data Protection Officer has carried out risk assessments that take into account all the circumstances of Connaught's controlling or processing operations.

In determining appropriateness, our Data Protection Officer has considered the extent of possible damage or loss that might be caused to individuals (e.g. staff or clients) if a security breach occurs, the effect of any security breach on Connaught itself, and any likely reputational damage including the possible loss of client trust. Considerations have included:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

3.8 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

Connaught demonstrates compliance with the data protection principles of the GDPR by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

4. Data subjects' rights

4.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- 4.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- 4.1.2 To prevent processing likely to cause damage or distress.
- 4.1.3 To prevent processing for purposes of direct marketing.
- 4.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- 4.1.5 To not have significant decisions that will affect them taken solely by automated process.
- 4.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
- 4.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- 4.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- 4.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- 4.1.10 To object to any automated profiling that is occurring without consent.

4.2 Connaught ensures that data subjects may exercise these rights:

- 4.2.1 Data subjects may make data access requests as described in our Subject Access Request Procedure; this procedure also describes how Connaught will ensure that its response to the data access request complies with the requirements of the GDPR.
- 4.2.2 Data subjects have the right to complain to Connaught related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with our Complaints Procedure.

5. Consent

5.1 Connaught understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

5.2 Connaught understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

5.3 Connaught gain consent from data subjects by the following means:

- 5.3.1 Information is collected via websites where an individual has made their data available and has consented to being contacted for the general purpose of recruitment services. This data is in the public domain and is usually taken from job boards;
  Information is collated from the websites and Job Boards where individuals will have posted their CV as part of their activity to find a new position or test their potential demand in the job market.
- 5.3.2 Connaught will contact a data subject to discuss the services that it can offer to help the individual to achieve the kind of career outcome they are seeking. During the course of the phone call, Connaught will explicitly ask the data subject for consent to hold their data;

5.3.3 Data subjects who engage with Connaught for services will be contacted by email to explicitly explain the collection of data and the purposes of processing, including the sharing of data with third parties.

5.4 Connaught do not collect special categories of personal data, as described in Article 9 of the GDPR. Connaught do not collect data related to children and do not collect data regarding criminal convictions. Connaught do not collect data related to credit cards or bank details. None of these types of data are necessary for Connaught to provide its services to data subjects.

6. Security of data

6.1 All staff at Connaught are responsible for ensuring that any personal data that Connaught holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Connaught to receive that information and has entered into a confidentiality agreement.

6.2 Access to personal data is given on a 'least privilege' basis to ensure that only those who need to use it are given access. All personal data is kept secure by the following means:

- if computerised, password protected in line with best practice; and
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media;
- if data is held in hard copy, it is stored in a lockable room with controlled access; and
- in a locked drawer or filing cabinet.

6.3 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs will be removed and immediately destroyed before disposal.

6.4 Connaught understands that processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

7. Disclosure of data

7.1 Connaught has provided awareness and training that ensures that personal data is not disclosed to unauthorised third parties.

7.2 Any requests received by Connaught to provide data to a third party in accordance with Article 23 of the GDPR must be supported by appropriate paperwork and all such disclosures must be specifically authorised by our Data Protection Officer.

8. Retention and disposal of data

8.1 Connaught shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

8.2 Connaught may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

8.3 The retention period for each category of personal data is set out in Connaught's Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations Connaught has to retain the data.

8.4 Connaught's data retention and data disposal procedures will apply in all cases.

8.5 Personal data will be disposed of securely in accordance with the sixth principle of the GDPR – *processed in an appropriate manner to maintain security*, thereby protecting the "rights and freedoms" of data subjects.

9. Data transfers

9.1 Connaught do not transfer data to any third parties outside of the European Economic Area (EEA).

10. Information asset register/data inventory

10.1 Connaught has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Connaught's data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of Connaught throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

10.2 Connaught assesses the level of risk to individuals associated with the processing of their personal data.

10.2.1 Data protection impact assessments (DPIAs) are carried out where appropriate in relation to the processing of personal data by Connaught, and in relation to processing undertaken by any other organisations on behalf of Connaught.

10.2.2 Connaught shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this notice.

10.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Connaught shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

10.2.4 Where, as a result of a DPIA it is clear that Connaught is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Connaught may proceed will be escalated for review to our Data Protection Officer.

10.2.5 Our Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

10.2.6 On an ongoing basis, appropriate controls will be selected utilising best practice principles and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of the GDPR.

11. Supervisory Authority Contact

You can obtain further information about your rights or make a complaint to your data protection authority with regards to how we use your information, and this section provides contact details should you need them.

Details of the UK supervisory authority: The Information Commissioner's Office. You can contact them in the following ways:

Phone: 0303 123 1113

Email: casework@ico.org.uk

Post: Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF